United States Government Accountability Office

GAO

Report to Congressional Committees

October 2009

DEFENSE CRITICAL INFRASTRUCTURE

Actions Needed to Improve the Identification and Management of Electrical Power Risks and Vulnerabilities to DOD Critical Assets

GAO-10-147

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
OCT 2009		**00-00-2009 to 00-00-2009**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Defense Critical Infrastructure. Actions Needed to Improve the Identificaiton and Management of Electrical Power Risks and Vulnerabilities to DOD Critical Assets	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Government Accountability Office,441 G Street NW,Washington,DC,20548**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**91**	

Contents

Table

Figures

Abbreviations

ASD(HD&ASA)	Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs
DCIP	Defense Critical Infrastructure Program
DHS	Department of Homeland Security
DISLA	Defense Infrastructure Sector Lead Agent
DOD	Department of Defense
DOE	Department of Energy

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

October 23, 2009

Congressional Committees

The Department of Defense (DOD) relies on a global network of defense critical infrastructure so essential that the incapacitation, exploitation, or destruction of an asset within this network could severely affect DOD's ability to deploy, support, and sustain its forces and operations worldwide and to implement its core missions, including those in Iraq and Afghanistan as well as its homeland defense and strategic missions. In October 2008, DOD identified its 34[1] most critical assets in this network—assets of such extraordinary importance to DOD operations that according to DOD, their incapacitation or destruction would have a very serious, debilitating effect on the ability of the department to fulfill its missions. Located both within the United States and abroad, DOD's most critical assets include both DOD- and non-DOD-owned assets.

DOD relies overwhelmingly on commercial electrical power grids[2] for secure, uninterrupted electrical power supplies to support its critical assets. DOD is the single largest consumer of energy in the United States, as we have noted in previous work.[3] According to a 2008 report by the Defense Science Board Task Force on DOD's Energy Strategy,[4] DOD has traditionally assumed that commercial electrical power grids are highly reliable and subject to only infrequent (generally weather-related), short-

[1] Although DOD's validated list of its most critical assets totals 29 assets, for purposes of this report, we refer to 34 most critical assets, since 4 of them have several components. Together, these components represent a larger capability, which constitutes the most critical asset.

[2] The U.S. commercial electrical power grid is a system of synchronized power providers and consumers connected by transmission and distribution lines and operated by one or more control centers. The U.S. power grid serving the contiguous 48 states is composed of three distinct power grids, or "interconnections"—the Eastern Interconnection, the Western Interconnection, and the Electric Reliability Council of Texas Interconnection. These interconnections provide power to the continental United States, Canada, and a small portion of northern Mexico.

[3] GAO, *Defense Management: Overarching Organizational Framework Needed to Guide and Oversee Energy Reduction Efforts for Military Operations*, GAO-08-426 (Washington, D.C.: Mar. 13, 2008).

[4] Defense Science Board, *Report of the Defense Science Board Task Force on DOD Energy Strategy, "More Fight—Less Fuel"* (Washington, D.C., February 2008).

term disruptions. For backup supplies of electricity, DOD has depended primarily on diesel generators with short-term fuel supplies.

In 2008, however, the Defense Science Board reported that "[c]ritical national security and homeland defense missions are at an unacceptably high risk of extended outage from failure of the [commercial electrical power] grid" upon which DOD overwhelmingly relies for its electrical power supplies. Specifically, the reliability and security of commercial electrical power grids are increasingly threatened by a convergence of challenges, including increased user demand, an aging electrical power infrastructure, increased reliance on automated control systems that are susceptible to cyberattack, the attractiveness of electrical power infrastructure for terrorist attacks, long lead times for replacing key electrical power equipment, and more frequent interruptions in fuel supplies to electricity-generating plants. As a result, commercial electrical power grids have become increasingly fragile and vulnerable to extended disruptions that could severely impact DOD's most critical assets, their supporting infrastructure, and ultimately the missions they support.

DOD addresses risk and vulnerabilities[5]—including those associated with electrical power—to its critical assets and installations through a variety of mission assurance–related programs.[6] In particular, as we have previously reported,[7] DOD has been responsible since September 2003 for developing and ensuring implementation of defense critical infrastructure protection policy and program guidance. To identify and help assure the availability of this mission-critical infrastructure, in August 2005 DOD established the Defense Critical Infrastructure Program (DCIP), assigning overall responsibility for the program to the Office of the Assistant

[5] For purposes of this report, we are using "risk" and "vulnerability" as defined in DOD Directive 3020.40, *Defense Critical Infrastructure Program (DCIP)* (Aug. 19, 2005). The directive defines "risk" as the probability and severity of loss linked to threats and hazards and defines "vulnerability" as the characteristics of an installation, system, asset, application, or its dependencies that could cause it to suffer a degradation or loss (incapacity to perform its designated function) as a result of having been subjected to a certain level of threat or hazard.

[6] While DOD acknowledges that the execution of its missions depends heavily on ensuring the availability of electrical power to installations with critical assets, DOD is not responsible for improving the reliability of the commercial electrical power grid.

[7] GAO, *Defense Infrastructure: Actions Needed to Guide DOD's Efforts to Identify, Prioritize, and Assess Its Critical Infrastructure*, GAO-07-461 (Washington, D.C.: May 24, 2007). Also, see Related GAO Products at the end of this report.

Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD(HD&ASA)).[8] Since then, ASD(HD&ASA) has issued formal DCIP program guidance, including a directive articulating the roles and responsibilities of relevant DOD organizations;[9] an instruction on program management;[10] and several program manuals, including ones on identifying critical assets and remediating asset risks and vulnerabilities.[11] Under DCIP, DOD also established 10 functionally based defense sectors—including one for public works, which encompasses electrical power infrastructure—and designated a Defense Infrastructure Sector Lead Agent (DISLA) for each sector.[12] In addition to using DCIP, DOD can also assess risks and vulnerabilities to its critical assets and installations (at the departmental, combatant command, military service, and installation levels) through other mission assurance programs and efforts, including those related to force protection; antiterrorism; defense continuity; information assurance; continuity of operations; chemical, biological, radiological, nuclear, and high-explosive defense; readiness; and installation preparedness. In addition, within the framework of the *National Infrastructure Protection Plan of 2009*,[13] DOD also collaborates with the Department of Homeland Security (DHS) and the Department of Energy (DOE) to address risks and vulnerabilities associated with electrical power infrastructure.

[8] Earlier programs analogous to DCIP can be traced back to 1998.

[9] DOD Directive 3020.40, *Defense Critical Infrastructure Program (DCIP)* (Aug. 19, 2005).

[10] DOD Instruction 3020.45, *Defense Critical Infrastructure Program (DCIP) Management* (Apr. 21, 2008).

[11] DOD Manual 3020.45, Volume 1, *Defense Critical Infrastructure Program (DCIP) DOD Mission-Based Critical Asset Identification Process (CAIP)* (Oct. 24, 2008), and DOD Manual 3020.45, Volume 2, *Defense Critical Infrastructure Program (DCIP) DCIP Remediation Planning* (Oct. 28, 2008).

[12] The 10 defense sectors are the Defense Industrial Base; Financial Services; Global Information Grid; Health Affairs; Intelligence, Surveillance, and Reconnaissance; Logistics; Personnel; Public Works; Space; and Transportation.

[13] The *National Infrastructure Protection Plan* is a risk management framework intended to protect the nation's critical infrastructures and key resources. This framework is composed of 18 critical infrastructure and key resource sectors, including an Energy Sector. According to the Energy Sector Specific Plan, the Energy Sector is composed of three subsectors (petroleum, natural gas, and electricity). The Department of Energy is the Sector-specific Agency tasked with implementing the framework and developing guidance tailored to the specific characteristics and risks associated with the Energy Sector.

In its May 2008 report on H.R. 5658,[14] the House Committee on Armed Services noted the risks of electrical power disruptions to critical DOD missions and, among other things, directed that GAO continue its review of DCIP.[15] In response to this mandate, we have examined (1) the extent to which DOD's most critical assets are vulnerable to disruptions in electrical power supplies and (2) the extent to which DOD—both within and outside of the Defense Critical Infrastructure Program—has attempted to assure the availability of electrical power supplies to its most critical assets.

We have previously conducted an extensive body of work on DOD's efforts to assure the availability of defense critical infrastructure, reporting on DOD's progress in addressing the evolving management framework for DCIP; coordination among DCIP stakeholders; implementation of key program elements; availability of public works infrastructure; and reliability issues in DOD's lists of critical assets, among other issues. We have also issued reports concerning federal critical infrastructure protection, cybersecurity, and electrical power. A list of these reports by category can be found at the end of this report in the Related GAO Products section.

To address our objectives in this report, we conducted three structured written surveys regarding the electrical power vulnerabilities of DOD's 34 most critical assets, which DOD identified through DCIP as of October 2008. We pretested the survey with U.S. Army, U.S. Navy, and U.S. Air Force officials representing three most critical asset sites as well as officials from the Joint Staff (J-34) and ASD(HD&ASA) to ensure that the questions were relevant, clearly stated, and easy to understand. We then administered one survey to the military services and DOD agencies that own or have program responsibility for the assets[16] through DCIP to obtain information about the assets' reliance on electrical power; the assets' primary and backup sources of electrical power supplies; the number and

[14] H.R. Rep. No. 110-652, pp. 523-524 (May 16, 2008).

[15] In this same report, the House Committee on Armed Services also directed the Secretary of Defense to complete an assessment of corrective actions required to provide assured power and secure and maintain redundancy of DOD's Tier 1 critical assets. DOD was directed to submit the report to the congressional defense committees by March 1, 2009; however, DOD notified the House Committee on Armed Services in April 2009 that because of the number of Tier 1 assets and the pace of the vulnerability assessments, the report would not be completed and delivered until September 2010.

[16] For non-DOD-owned most critical assets, DOD organizations may be called asset owners because of their DCIP risk management responsibilities for those assets.

type of unplanned electrical power disruptions to the assets; DCIP and non-DCIP assessments of the assets' risks and vulnerabilities to electrical power disruptions from January 2006 through December 2008; and measures recommended, implemented, or planned to address or manage such risks and vulnerabilities.[17] We administered another survey to the Joint Staff to obtain information about the missions supported by the assets. Finally, we administered the third survey to ASD(HD&ASA) regarding coordination efforts with relevant DOD and non-DOD stakeholders. (These surveys are reproduced in full in apps. III, IV, and V.) We also conducted six follow-up site visits to a nonprobability sample of critical assets to verify and validate the surveys' results and evaluate in-depth issues identified in the surveys' responses, including vulnerability assessments.

We also interviewed and obtained information from officials representing ASD(HD&ASA)/DCIP Office, the Joint Staff's Directorate for Antiterrorism and Homeland Defense, the U.S. Air Force, the U.S. Army, the U.S. Navy, the U.S. Marine Corps, the U.S. Army Corps of Engineers, the Defense Threat Reduction Agency, the Mission Assurance Division of the Naval Surface Warfare Center, the Defense Science Board's Task Force on DOD Energy Security, selected DOD installations, DHS, DOE, the Federal Energy Regulatory Commission, the North American Electric Reliability Corporation, the Edison Electrical Institute, and other private-sector energy organizations.

As agreed with staff of the House Committee on Armed Services, in addition to issuing this unclassified report, we are issuing a separate classified product.

[17] We planned to select a random sample of DOD Tier 1 Task Critical Assets—which support critical DOD missions at the departmental, combatant command, and military service levels—to survey for this review. These assets represent DOD's second most important group of critical assets. However, our discussions with DOD officials and our own analysis led us to determine that the DOD-identified universe of critical assets did not represent an accurate, comprehensive list of DOD Tier 1 Task Critical Assets, and that this issue in and of itself warranted further analysis. Therefore, we issued a separate report, with recommendations, on issues relating specifically to the Tier 1 Task Critical Asset list to enable DOD to take timely actions to update and improve its list of Defense Critical Assets in the fall of 2009 and prioritize funding. See GAO, *Defense Critical Infrastructure: Actions Needed to Improve the Consistency, Reliability, and Usefulness of DOD's Tier 1 Task Critical Asset List*, GAO-09-740R (Washington, D.C.: July 17, 2009).

We conducted this performance audit from October 2008 through October 2009 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. A more thorough description of our scope and methodology is provided in appendix I.

Results in Brief

DOD's most critical assets are vulnerable to disruptions in electrical power supplies, but DOD lacks sufficient information to determine the full extent of the risks and vulnerabilities these assets face. All 34 of these most critical assets require electricity continuously to support their military missions, and 31 of them rely on commercial power grids—which the Defense Science Board Task Force on DOD Energy Strategy has characterized as increasingly fragile and vulnerable—as their primary source of electricity. DOD Instruction 3020.45 requires DOD to conduct vulnerability assessments on all its most critical assets at least once every 3 years. Also, ASD(HD&ASA) has requested the U.S. Army Corps of Engineers—which serves as the Defense Critical Infrastructure Program's Defense Infrastructure Sector Lead Agent for Public Works—to conduct preliminary technical analyses of DOD installation infrastructure (including electrical power infrastructure) to support the teams conducting Defense Critical Infrastructure Program vulnerability assessments on the most critical assets.

- As of June 2009, and according to ASD(HD&ASA) and the Joint Staff, DOD had conducted Defense Critical Infrastructure Program vulnerability assessments on 14 of the 34 most critical assets.[18] DOD has not conducted the remaining assessments because it did not identify the most critical assets until October 2008. To comply with the instruction, DOD would have to complete Defense Critical Infrastructure Program vulnerability assessments on all most critical assets by October 2011.
- DOD has neither conducted, nor developed additional guidelines and time frames for conducting, these vulnerability assessments on any of the five non-DOD-owned most critical assets located in the United

[18] DOD began conducting DCIP assessments in 2007 on selected DOD Task Critical Assets, some of which were subsequently designated as DOD's most critical assets in October 2008.

States or foreign countries, citing security concerns and political sensitivities.

- The U.S. Army Corps of Engineers has not completed the preliminary technical analyses requested because it has not yet received infrastructure-related information regarding the networks, assets, points of service, and inter- and intradependencies related to electrical power systems that it requires from the military services.
- Although DOD is in the process of developing guidelines, it does not systematically coordinate Defense Critical Infrastructure Program vulnerability assessment processes and guidelines with those of other, complementary DOD mission assurance programs—including force protection; antiterrorism; information assurance; continuity of operations; chemical, biological, radiological, nuclear, and high-explosive defense; readiness; and installation preparedness—that also examine electrical power vulnerabilities of the most critical assets, because DOD has not established specific guidelines for such systematic coordination.
- The 10 Defense Critical Infrastructure Program vulnerability assessments we reviewed did not explicitly consider assets' vulnerabilities to longer-term (i.e., of up to several weeks' duration) electrical power disruptions[19] on a mission-specific basis, as DOD has not developed explicit Defense Critical Infrastructure Program benchmarks for assessing electrical power vulnerabilities associated with longer-term electrical power disruptions.

With more comprehensive knowledge of the most critical assets' risks and vulnerabilities to electrical power disruptions, DOD can better avoid compromising crucial DOD-wide missions during electrical power disruptions. This additional information may also improve DOD's ability to effectively prioritize funding needed to address identified risks and vulnerabilities of its most critical assets to electrical power disruptions.

While DOD has taken some steps toward assuring the availability of its electrical power supplies to its most critical assets, it lacks a mechanism

[19] Definitions of "longer-term" or "extended" electrical power disruptions vary. For example, in the January 2008 report, The MITRE Corporation, Power Grid Security, JSR-07-125 (McLean, Va., January 2008), which was requested by DHS, the JASON Program Office of The MITRE Corporation defined a catastrophic, long-term failure of the electrical power grid as one lasting 5 days or longer. In contrast, in the *Report of the Defense Science Board Task Force on DOD Energy Strategy*, the Defense Science Board refers to a "long term outage" as lasting "several months." DOD officials also noted that the duration of a longer-term or extended electrical power disruption for a specific asset varies depending on the nature of the particular mission(s) supported by that asset.

for tracking the implementation of future Defense Critical Infrastructure Program risk management decisions and responses, and its coordination with local electricity providers has been limited. From August 2005 through October 2008, DOD issued Defense Critical Infrastructure Program guidance for identifying critical assets, assessing their vulnerabilities, and making risk management decisions about those vulnerabilities. In addition, DOD has conducted various types of vulnerability assessments—including Defense Critical Infrastructure Program vulnerability assessments, Joint Staff Integrated Vulnerability Assessments, and other mission assurance–related assessments—on 24 of the most critical assets, including multiple assessments on some of the same assets. According to the survey, these Defense Critical Infrastructure Program and other DOD vulnerability assessments have identified various electrical power vulnerabilities for 10 of the assets. DOD has also coordinated with other federal agencies—including DHS, DOE, and the Federal Energy Regulatory Commission—and industry organizations in an effort intended to assure the availability of electrical power supplies to the most critical assets. However, ASD(HD&ASA)—which has responsibility for overseeing the implementation of actions for the remediation, mitigation, or acceptance of risks to DOD critical assets—has not yet developed a mechanism to track the implementation of future Defense Critical Infrastructure Program risk management decisions, along with responses intended to address risks and vulnerabilities identified for the most critical assets. Without such information, DOD cannot comprehensively determine whether asset owners are taking the necessary steps to address identified risks and vulnerabilities of all of the most critical assets to electrical power disruptions. In addition, Defense Critical Infrastructure Program guidance encourages coordination between DOD installations with critical assets and their respective public utilities, including electricity providers, in order to remediate risks involving those utilities—for example, by discussing potential changes in service agreements with those utilities. However, according to our survey results, such coordination with local electricity providers has occurred for only 7 of DOD's 34 most critical assets. As a result, DOD may not be taking advantage of available expertise on electrical power issues from such providers. Without increased coordination between more DOD installations with critical assets and their respective local electricity providers, DOD potentially limits the risk mitigation or remediation options available to it for addressing the vulnerabilities of its most critical assets to electrical power disruptions.

We are recommending that DOD complete Defense Critical Infrastructure Program vulnerability assessments on all DOD-owned most critical assets;

develop additional guidelines, an implementation plan, and a schedule for conducting such assessments on all non-DOD-owned most critical assets; establish a time frame for the military services to provide the infrastructure data required to complete preliminary technical analysis of public works (including electrical system) infrastructure at DOD installations that support DOD's most critical assets; finalize guidelines to coordinate Defense Critical Infrastructure Program assessment criteria and processes more systematically with those of other DOD mission assurance programs; develop Defense Critical Infrastructure Program guidelines for assessing the most critical assets' vulnerabilities to longer-term electrical power disruptions; develop a mechanism to track the implementation of future Defense Critical Infrastructure Program risk management decisions; and ensure or facilitate that asset owners and host installations of the most critical assets reach out to local electricity providers to coordinate and help remediate or mitigate risks and vulnerabilities to electrical power disruptions.

DOD concurred with all of our recommendations. Based on DOD's comments, we modified our original recommendation that the department establish a time frame for the military services to provide infrastructure data required by the Public Works Defense Infrastructure Sector Lead Agent (the U.S. Army Corps of Engineers) to conduct preliminary technical analysis of public works (including electrical system) infrastructure at DOD installations that support DOD's most critical assets. According to DOD, the U.S. Army Corps of Engineers has already completed this technical analysis for public works infrastructure located outside of the installations, but is still waiting for the military services to provide data required to complete the analysis on infrastructure located within the installations. As a result, our final recommendation indicates that these data are required for completing, rather than conducting, the preliminary technical analysis.

Background

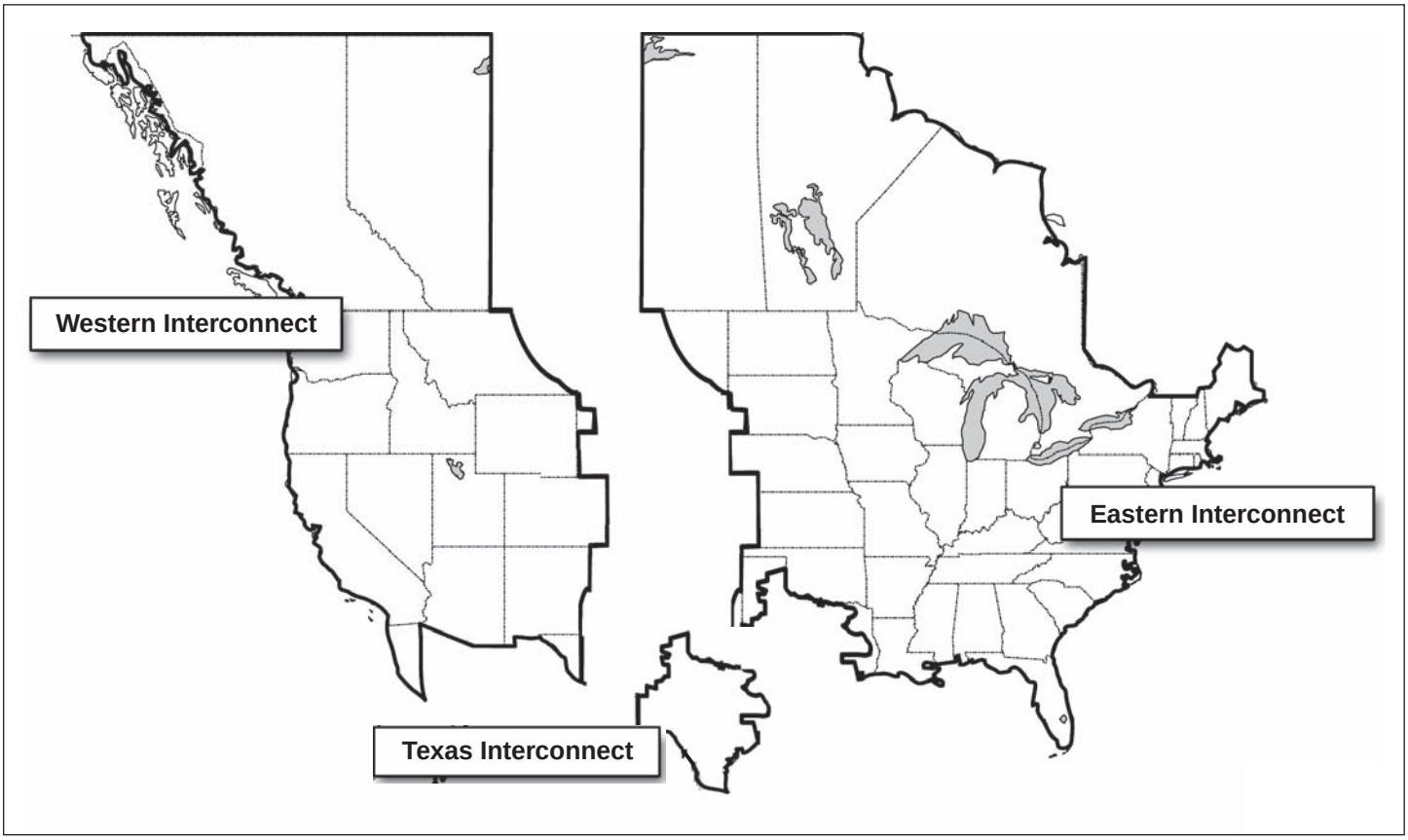
DOD's Vulnerability to Electrical Power Disruptions

DOD depends overwhelmingly on the U.S. commercial electrical power grid for electricity to support its operations and missions.[20] As illustrated in figures 1 and 2, the grid is a vast, complex network of interconnected regional systems and infrastructure (e.g., power plants, electricity lines, and control centers) used to generate, transmit, distribute, and manage electrical power supplies across the United States. According to the Defense Science Board Task Force on DOD Energy Strategy, approximately 99 percent of the electrical power DOD installations consume originates from outside installation boundaries, while approximately 85 percent of the energy infrastructure that DOD relies on for electrical power is commercially owned and outside of DOD's control.[21]

[20] For more information about the U.S. commercial electrical power grid, see GAO, *Electricity Restructuring: 2003 Blackout Identifies Crisis and Opportunity for the Electricity Sector*, GAO-04-204 (Washington, D.C.: Nov. 18, 2003).

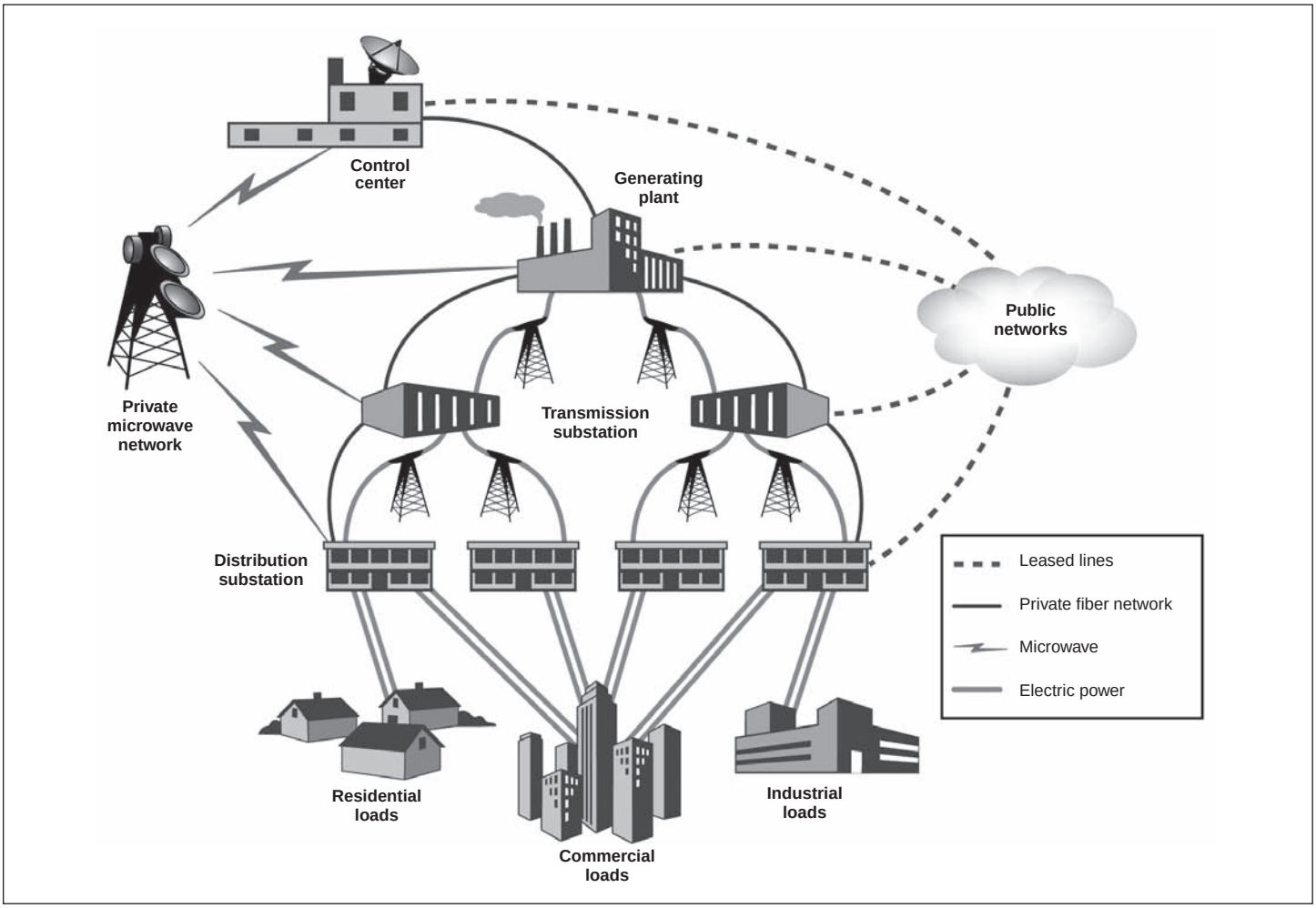
[21] Defense Science Board, *Report of the Defense Science Board Task Force on DOD Energy Strategy, "More Fight—Less Fuel."*

Figure 1: The U.S. Commercial Electrical Power Grid Interconnects



Sources: GAO-04-204 and North American Electric Reliability Corporation.

Figure 2: Overview of the Electric Power System and Control Communications



Source: DOE, *Energy Sector Specific Plan* (May 2007).

There are currently a variety of mechanisms in place that may help to mitigate the risk of losing electricity service due to electrical power disruptions, including mandatory reliability standards for the electrical power industry approved by the Federal Energy Regulatory Commission. In addition, other risk mitigation measures are being considered, such as islanding.[22] However, while the U.S. commercial electrical power grid is

[22] The concept of islanding entails the isolation of critical loads or entire installations from the grid to make them self-sufficient.

generally a reliable source of electricity and is subject to some reliability standards that typically assure its availability over 99 percent of the time, concerns have been raised about the increasing vulnerability of the grid to more frequent or longer electrical power disturbances. For example, the Defense Science Board Task Force reported that the commercial power grid is "brittle, increasingly centralized, capacity-strained, and largely unprotected from physical attack, with little stockpiling of critical hardware." Similarly, according to the May 2007 *Infrastructure Resiliency Guide* for DOD's Defense Critical Infrastructure Program, "the electric power network is a complex system of interconnected components that can fail and cause massive service disruptions." Factors that contribute to the grid's vulnerability include (1) increasing national demand for electricity; (2) an aging electrical power infrastructure; (3) increased reliance on automated control systems that are susceptible to cyberattacks; (4) the attractiveness of electrical power infrastructure as targets for physical or terrorist attacks; (5) long lead times (of several months to several years) for replacing high-voltage transformers—which cost several millions of dollars and are manufactured only in foreign countries—if attacked or destroyed; and (6) more frequent interruptions in fuel supplies to electricity-generating plants.[23]

The National Science and Technology Council's Committee on Homeland and National Security also established a task force in January 2009 to identify research and development needs for electric grid vulnerabilities and to coordinate with other federal agencies to address those needs.[24] In addition, government and industry efforts are under way to examine

[23] For example, the stresses of increased demand for electrical power contributed to the 2003 Northeast Blackout, which was an extended cascading power outage that affected about 50 million people living in a 9,300 square mile area in the United States and Canada. More than 500 generating units at 265 power plants shut down during the outage, 22 of which were nuclear. It took over 2 weeks for power plants to regain full capacity. For additional information, see GAO-04-204.

[24] Members of the Task Force on Electric Grid Vulnerability represent DOD (co-chair), DOE (co-chair), DHS, the Director of National Intelligence, the Environmental Protection Agency, the Federal Energy Regulatory Commission, the National Aeronautics and Space Administration, the Nuclear Regulatory Commission, the Office of Science and Technology Policy, and the Office of Management and Budget.

cybersecurity threats, develop potential "Smart Grid"[25] solutions to address some of the grid's vulnerabilities, and develop and enforce electricity reliability standards for the industry.[26]

DOD assets are vulnerable to electrical power disruptions in various ways. For example, according to the *DCIP Infrastructure Resiliency Guide*,[27] vulnerabilities may involve the co-location of both primary and secondary electrical power equipment, single points of failure in an electrical power network, lack of security access controls to critical electrical power equipment, electrical power lines sharing rights-of-way with other utilities, and insufficient backup sources of electrical power generation. To address such vulnerabilities, the guide suggests that owners or operators of DOD assets consider diversifying the locations of primary and secondary electrical power equipment, establishing independent transmission paths for commercial and backup electrical power, increasing security and monitoring access to critical electrical power equipment, establishing mitigation options based on potential loss of rights-of-way, and developing additional backup sources of electrical power. For more detailed

[25] Government and industry efforts to develop a "Smart Grid" are intended to modernize the aging U.S. electrical power transmission and distribution system, which uses technologies and strategies that are several decades old and include limited use of digital communication and control technologies. The Smart Grid would use advanced sensing, communication, and control technologies to generate and distribute electricity more effectively, economically, and securely. DOE's Office of Electricity Delivery and Energy Reliability calls for the Smart Grid to be more reliable, secure, economical, efficient, environmentally friendly, and safe, and expects it to enable active participation by consumers; accommodate a range of generation and storage options; enable new products, services, and markets; provide power quality for the digital economy; optimize asset utilization and operate efficiently; anticipate and respond to system disturbances; and operate resiliently against attacks and natural disasters. However, Smart Grid–related technologies may also introduce additional vulnerabilities to the U.S. electrical power grid, such as increased susceptibility to cyberattacks.

[26] For example, on July 21, 2009, the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology of the House Committee on Homeland Security held a hearing, "Securing the Modern Electric Grid from Physical and Cyber Attacks." Similarly, on July 23, 2009, the Subcommittee on Energy and Environment of the House Committee on Science and Technology held a hearing, "Effectively Transforming Our Electric Delivery System to a Smart Grid." In addition, as discussed later in this background section, the Federal Energy Regulatory Commission has approved reliability standards for the electrical power industry, which may be enforced by either the Federal Energy Regulatory Commission or the North American Electric Reliability Corporation.

[27] Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs, *Defense Critical Infrastructure Program Infrastructure Resiliency Guide: Reduce Your Vulnerabilities and Make Your Infrastructure Stronger*, Version 1.0 (Washington, D.C., May 2007).

information regarding typical electrical power vulnerabilities that could affect DOD assets and potential measures to address them, see appendix II.

DCIP

DOD identifies the vulnerabilities and manages the risks of its most critical assets to electrical power disruptions primarily through DCIP. On October 14, 2008, DOD designated 34[28] assets through DCIP as its most critical assets—assets of such extraordinary importance to DOD operations that according to DOD, their incapacitation or destruction would have a very serious, debilitating effect on the ability of the department to fulfill its missions. While most (29 of 34) of these critical assets—which may be located in the United States, U.S. territories, or foreign countries—are owned by DOD, 5 are owned by other entities, including both domestic and foreign commercial and other governmental entities. To ensure the availability of these and other networked assets critical to DOD missions, DCIP uses a risk management model that helps decision makers (1) identify the department's critical assets based on the criticality of their missions; (2) conduct "threat and hazard assessments;" (3) conduct "vulnerability assessments" (that include detailed reviews of electrical power vulnerabilities); (4) conduct "risk assessments" to determine the consequences of the assets' loss, evaluate the importance and urgency of proposed actions, and develop alternate courses of action; (5) reach "risk management decisions" to accept risks or reduce risks to acceptable levels; and (6) formulate "risk responses" to implement the risk management decisions.[29]

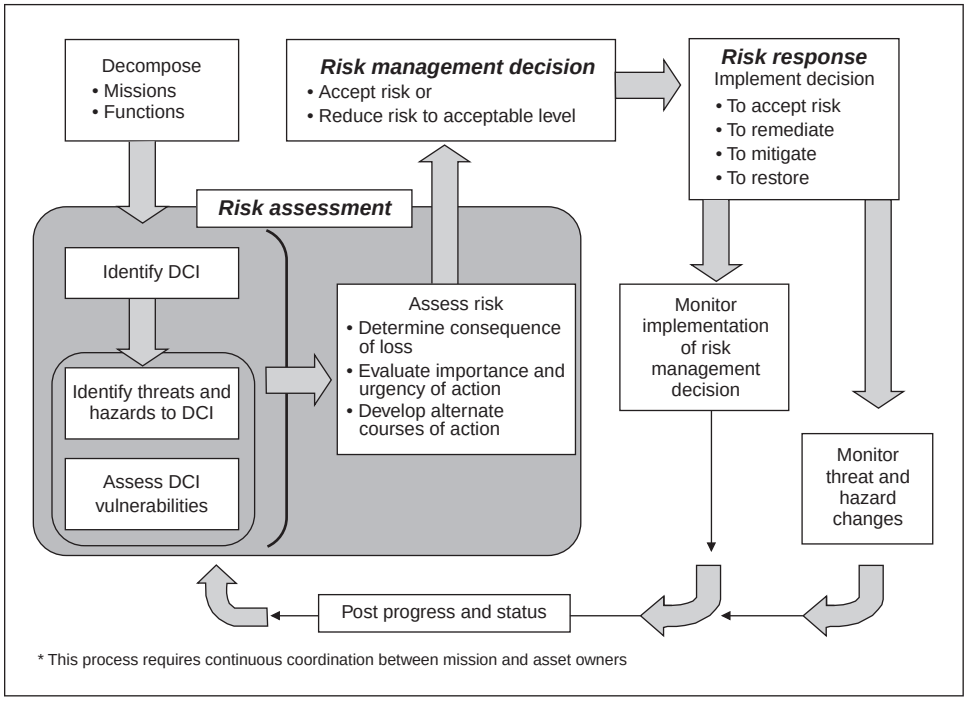
[28] See footnote 1 regarding the number of most critical assets.

[29] DCIP guidance defines a "threat" as an adversary having the intent, capability, and opportunity to cause loss or damage, and a "hazard" as a nonhostile incident, such as an accident, natural force, or technological failure, that causes loss or damage to an asset. DCIP defines a "vulnerability" as a characteristic of an installation, system, asset, application, or its dependencies that could cause it to suffer a degradation or loss (incapacity to perform its designated function) as a result of having been subjected to a certain level of threat or hazard. A "risk response" may involve DCIP stakeholders accepting an identified risk or applying funding and resources to reduce the risk (i.e., remediation); to minimize the effects of potential threats or hazards (i.e., mitigation); or to restore lost capacity in the aftermath of an event (i.e., reconstitution). A risk response is intended to ensure that limited resources are optimally allocated toward those assets that are most important to DOD's overall mission success and for which an identified level of risk is deemed unacceptable.

Key stakeholders involved in these DCIP processes include ASD(HD&ASA), which serves as the principal civilian advisor to the Secretary of Defense on the identification, prioritization, and protection of defense critical infrastructure; the Chairman of the Joint Chiefs of Staff, who serves as DOD's principal military advisor for the program; and the combatant commands, the military services, and other DOD agencies and organizations, which may serve as asset owners or mission owners for specific critical assets.[30] In addition, as the DISLA for the DCIP Public Works Defense Sector—which includes both DOD-owned and non-DOD assets used to support, generate, produce, or transport electrical power for and to DOD users—the U.S. Army Corps of Engineers is responsible for identifying asset interdependencies in its sector, including those related to electrical power, as appropriate. Figure 3 illustrates the key elements of the DCIP risk management model.

[30] ASD(HD&ASA), within the Office of the Under Secretary of Defense for Policy, serves as the principal civilian advisor, and the Chairman of the Joint Chiefs of Staff serves as the principal military advisor to the Secretary of Defense on critical infrastructure protection. ASD(HD&ASA) has lead responsibility for developing and ensuring the implementation of DCIP policy and program guidance for the identification, prioritization, and protection of defense critical infrastructure.

Figure 3: Key Elements of DCIP Risk Management



Source: DOD Instruction 3020.45.

Note: The DCIP Risk Management process begins with the combatant commands, military services, and Defense Infrastructure Sector Lead Agents decomposing (i.e., identifying and analyzing) their missions and functions to identify defense critical infrastructure (DCI).

Other Risk Management Programs and Activities in DOD

In addition to using DCIP, DOD also identifies vulnerabilities and manages the risks of its most critical assets, including those related to electrical power, through other DOD mission assurance programs or activities, including those related to force protection; antiterrorism; information assurance; continuity of operations; chemical, biological, radiological, nuclear, and high-explosive defense; readiness; and installation preparedness. These programs and activities are intended to ensure that required capabilities and supporting infrastructures are available to DOD to carry out the *National Military Strategy*.[31] DOD has established several complementary programs that help protect critical assets, including those

[31] Mission assurance links numerous risk management program activities and security-related functions to create the synergistic effect required for DOD to mobilize, deploy, support, and sustain military operations throughout the continuum of operations.

listed in table 1. In addition, the military departments have developed service-level critical infrastructure protection programs, which they coordinate with DCIP.[32]

Table 1: Summary of Selected DOD Mission Assurance Programs

Program	Mission assurance emphasis
Antiterrorism Program	Establish standards for DOD assets to protect them against acts of terrorism.[a]
Department of Defense Continuity Programs[b]	Ensure that DOD mission-essential functions continue under all circumstances across the spectrum of threats.[c]
Information Assurance Program	Ensure that essential DOD information systems maintain an appropriate level of confidentiality, integrity, authenticity, nonrepudiation, and availability.[d]
Installation Emergency Management Program	Prepare DOD installations for emergencies by using a comprehensive all-hazards approach to protect personnel and save lives, and recover and restore operations after an emergency.[e]
Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive Emergency Response Guidelines	Prepare DOD installation emergency responders for the effects of a chemical, biological, radiological, nuclear, or high explosive incident to preserve life, prevent human suffering, mitigate incidents, and protect critical assets and infrastructure.[f]

Source: GAO analysis of DOD guidance.

[a]DOD Directive 2000.12, *DOD Antiterrorism (AT) Program* (Washington, D.C., Aug. 18, 2003, certified current as of Dec. 13, 2007).

[b]DOD Directive 3020.40 calls for DCIP to complement DOD's continuity of operations program, which is addressed as part of DOD's Defense Continuity Programs.

[c]DOD Directive 3020.26, *Department of Defense Continuity Programs (DCP)* (Washington, D.C., Jan. 9, 2009).

[d]DOD Directive 8500.01E, *Information Assurance Program (IA)* (Washington, D.C., Oct. 24, 2002; certified current as of Apr. 23, 2007).

[e]DOD Instruction 6055.17, *DOD Installation Emergency Management Program (IEM)* (Washington, D.C., Jan. 13, 2009).

[f]DOD Instruction 2000.18, *Department of Defense Installation Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive Emergency Response Guidelines (CBRNE)* (Washington, D.C., Dec. 4, 2002).

[32] For example, the military departments have also conducted service-level Critical Asset Risk Assessments on some of the most critical assets.

Other Agencies and Organizations with Roles in Risk Management

Other federal agencies and industry organizations are to collaborate with DOD and play significant roles in protecting critical electrical power infrastructure within the framework of Homeland Security Presidential Directive 7. This directive, issued in December 2003, requires all federal departments and agencies to identify, prioritize, and coordinate the protection of critical infrastructure and key resources from terrorist attacks.[33] These entities and their roles are summarized below.

Department of Homeland Security. DHS is the principal federal entity responsible for leading, integrating, and coordinating the overall national effort to protect the nation's critical infrastructure and key resources. DHS led the development of the National Infrastructure Protection Plan, which provides a framework for managing risks to U.S. critical infrastructure and outlines the roles and responsibilities of DHS and other security partners—including other federal agencies; state, territorial, local, and tribal governments; and private companies.[34] DHS is responsible for leading and coordinating a national effort to enhance protection through 18 critical infrastructure and key resource sectors,[35] and a "sector-specific agency" has lead responsibility for coordinating the protection of each of the sectors.

Department of Energy. DOE serves as the sector-specific agency for the Energy Sector, which includes critical infrastructure and key resources related to electricity. DOE is responsible for developing an Energy Sector Specific Plan, in close collaboration with other National Infrastructure Protection Plan stakeholders, that applies the plan's risk management model to critical infrastructure and key resources within that sector. Within DOE, the Office of Electricity Delivery and Energy Reliability seeks to lead national efforts to modernize the electrical grid; enhance security and reliability of energy infrastructure; and facilitate

[33] Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection* (Washington, D.C., Dec. 17, 2003).

[34] Department of Homeland Security, *National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency, 2009* (Washington, D.C., 2009).

[35] The *National Infrastructure Protection Plan* designates 18 sectors to focus on specific categories of critical infrastructure and key resources—including one for Energy and another one for the Defense Industrial Base—and assigns a federal agency to lead each sector.

recovery from disruptions to energy supply. When requested, DOE and its national laboratories[36] can provide energy-related expertise and assistance to DOD. According to DOE officials, DOE and several DOD combatant commands, including U.S. European Command and U.S. Africa Command, are considering utilizing DOE representatives as energy attachés to those commands. The DOE representatives can provide energy-related expertise to their respective commands, particularly with respect to the commands' energy-related planning activities and the security and reliability of the commands' energy infrastructure.

Federal Energy Regulatory Commission and the North American Electric Reliability Corporation. The Energy Policy Act of 2005 provided the Federal Energy Regulatory Commission[37] and its subsequently appointed Electric Reliability Organization—the North American Electric Reliability Corporation[38]—new responsibilities for helping protect and improve the reliability and security of the U.S. bulk power system[39] through the establishment, approval, and enforcement of mandatory electrical reliability standards.[40] Both of these organizations also participate in safeguarding the nation's critical infrastructures and key resources, and they have interacted with DOD regarding electrical power

[36] DOE"s system of 17 national laboratories performs research and development that is not well-suited to university or private-sector research facilities because of its scope, infrastructure, or multidisciplinary nature, but for which there is a strong public and national need.

[37] The Federal Energy Regulatory Commission is an independent federal agency that regulates the interstate transmission of electricity, natural gas, and oil, and oversees the reliability of high-voltage interstate transmission systems, among other responsibilities.

[38] The North American Electric Reliability Corporation is an independent, self-regulatory, not-for-profit organization whose mission is to ensure the reliability of the bulk power system in North America.

[39] The bulk power system is that part of the power grid that includes the transmission of electricity over high-voltage transmission lines to distribution companies and the generation of electricity into those transmission lines. This includes most power generation facilities and most transmission lines over 100,000 volts, but excludes all distribution facilities.

[40] Reliability standards are the reliability requirements for planning and operating the North American bulk power system. The North American Electric Reliability Corporation's reliability standards for the bulk power system cover 14 areas, including critical infrastructure protection, emergency preparedness and operations, and protection and control.

vulnerabilities. Similarly, the North American Electric Reliability Corporation has collaborated with DOD and military service officials through the federal Task Force on Electric Grid Vulnerability, which is co-chaired by DOD, to identify and address electrical power vulnerabilities.

The Electrical Power Industry. Electrical power industry representatives also contribute to the assurance of electrical power supplies through industry associations—such as the Edison Electric Institute, the American Public Power Association, and the National Rural Electric Cooperative Association—and through local electrical power providers to DOD installations or assets. Electrical power industry associations, for example, collaborate with the federal government to help secure the U.S. electrical power grid through coordinating mechanisms in the National Infrastructure Protection Plan. In early 2009 the institute established the Energy Security Partnership Group, which includes officials from DOD installations and focuses on improving communications between DOD and its utilities and on identifying and removing barriers to the development of comprehensive energy security programs at DOD installations.

DOD's Most Critical Assets Are Vulnerable to Electrical Power Disruptions, but DOD Lacks Sufficient Information to Determine the Full Extent of Their Vulnerability

DOD's Most Critical Assets Rely on Electrical Power and Depend Overwhelmingly on Commercial Electrical Power Grids as Their Primary Supply

DOD's most critical assets and the missions they support are vulnerable to disruptions in electrical power supplies because of the extent of their reliance on electricity, particularly from the commercial electrical power grid. According to our survey of DOD's most critical assets, all of these assets require electrical power continuously in order to function and support their mission(s). Furthermore, the survey results indicate that all of the most critical assets depend on other supporting infrastructure—such as water; natural gas; and heating, ventilation, and air conditioning—that in turn also rely on electricity to function. As a result, without appropriate backup electrical power supplies or risk management measures, these critical assets may be unable to function fully and support their mission(s) in the event of an electrical power disruption. According to our survey, at least 24 of the 34 most critical assets experienced some electrical power disruptions—lasting up to 7 days—during the 3-year period from January 2006 through December 2008, and the missions supported by 3 of those critical assets were adversely impacted by electrical power disruptions. In addition, based on our survey, 31 of these 34 assets rely primarily on commercial electrical power grids for their electricity supplies. The U.S. commercial electrical power grids have become increasingly fragile and vulnerable to prolonged outages because of such factors as (1) increased user demand, (2) fewer spare parts for key electrical power equipment, (3) increased risks of deliberate physical or cyberattacks on electrical power infrastructure by terrorists, and (4) more frequent interruptions in fuel supplies to electricity-generating plants.[41]

[41] Defense Science Board, *Report of the Defense Science Board Task Force on DOD Energy Strategy, "More Fight—Less Fuel."*

Based on our survey, vulnerability assessments of 6 of the most critical assets reported vulnerabilities associated with the reliability of the electrical power grids of their commercial electricity providers or DOD installations. Furthermore, 8 of these critical assets attributed some of their electrical power disruptions to their commercial electrical power provider.

DOD Has Not Yet Completed DCIP Vulnerability Assessments on All of Its Most Critical Assets

DOD is identifying key vulnerabilities—including those related to electrical power—of its most critical assets through DCIP vulnerability assessments, but as of June 2009, the department had conducted such assessments on only 14 of its 34 most critical assets. As part of the DCIP risk management process, DCIP vulnerability assessments are intended to systematically examine the characteristics of an installation, system, asset, application, or its dependencies that could cause it to suffer a degradation or loss—that is, incapacity to perform its designated function—as a result of having been subjected to a certain level of threat or hazard. These vulnerability assessments—most of which the Defense Threat Reduction Agency has been conducting for DOD[42]—include specific reviews of the critical assets' supporting electrical power networks "to ensure that the distribution network at a given location and supporting offsite [electrical power] system has the capacity, redundancy, path diversity, security, survivability, and reliability to properly support a given mission."[43]

DOD Instruction 3020.45 requires DOD to conduct DCIP vulnerability assessments on all of its most critical assets at least once every 3 years. However, while DOD has conducted DCIP assessments on some of its most critical assets since March 2007, ASD(HD&ASA) and Joint Staff officials indicated that the department could not schedule or conduct these assessments systematically until its most critical assets were

[42] As of June 1, 2009, the Defense Threat Reduction Agency had conducted DCIP vulnerability assessments on 12 of the most critical assets as additional modules to its Joint Staff Integrated Vulnerability Assessments, which focus on antiterrorism and force protection vulnerabilities. The agency also conducted a DCIP vulnerability assessment on one most critical asset in conjunction with a Balanced Survivability Assessment. In addition, the U.S. Air Force conducted a DCIP vulnerability assessment on one other most critical asset as part of its service-level critical infrastructure protection program.

[43] Department of Defense, *DCIP Electrical Power Standards and Benchmarks*, Version 1.1 (Apr. 15, 2007).

formally identified in October 2008.[44] As a result, as of June 2009, DOD had conducted DCIP vulnerability assessments on 14 of the 34 most critical assets; had scheduled additional assessments for 13 other most critical assets from July 2009 through December 2010; and had not yet scheduled assessments for the remaining 7 most critical assets.[45] According to ASD(HD&ASA) and Joint Staff officials, DCIP vulnerability assessments will be conducted on all the most critical assets by October 2011, as required by DOD Instruction 3020.45. Nevertheless, until DOD completes these DCIP vulnerability assessments, the department will not have complete information about electrical power vulnerabilities for all the most critical assets.

DOD Lacks Additional Guidance for Conducting DCIP Vulnerability Assessments on Its Non-DOD-Owned Most Critical Assets

DOD has not yet conducted or scheduled DCIP vulnerability assessments, including assessments of electrical power vulnerabilities, on any of its non-DOD-owned most critical assets—both those located in the United States and in foreign countries—and has not yet developed guidance addressing the unique challenges related to conducting the assessments on such assets. While the majority of the most critical assets—which may be located in the United States, U.S. territories, or foreign countries—are owned by DOD, 5 of the 34 are not owned by DOD. Instead, such critical assets are owned by either U.S. or foreign commercial or governmental entities. DOD Instruction 3020.45 requires DOD to conduct DCIP vulnerability assessments at least once every 3 years on all of its most critical assets, regardless of the assets' ownership or location. However, DOD has not yet conducted or even scheduled DCIP vulnerability assessments for any of the non-DOD-owned most critical assets located in the United States or abroad. Furthermore, while DOD has issued extensive DCIP guidance applicable to all defense critical infrastructure (including non-DOD-owned critical infrastructure), as discussed above, DOD has not yet developed a systematic approach or guidelines addressing the unique challenges related to conducting the assessments on such non-DOD-owned critical assets. ASD(HD&ASA) and Joint Staff officials cited security concerns, political sensitivities, and lack of DOD authority over

[44] Before October 2008, the Defense Threat Reduction Agency conducted DCIP vulnerability assessments on assets that ASD(HD&ASA) and the Joint Staff considered to be likely candidates for the list of most critical assets.

[45] These remaining assets include five non-DOD-owned assets located in the United States and foreign countries, which are discussed in the following section of this report, and two DOD-owned assets located in the United States.

non-DOD-owned assets as key challenges in conducting the DCIP vulnerability assessments on the non-DOD-owned most critical assets in foreign countries. For example, according to these officials, notifying a U.S. or foreign commercial entity, or a foreign government, about its asset's designation as one of DOD's most critical assets could compromise DCIP security guidelines or U.S. national security. Similarly, for political reasons, foreign companies or governments may not want to have their assets identified as supporting U.S. or DOD military missions.

ASD(HD&ASA) and Joint Staff officials recognize the need for developing an approach and guidelines to conduct DCIP vulnerability assessments on the five non-DOD-owned most critical assets, particularly those located abroad. According to these officials, DOD has begun to coordinate with the Department of State's Office of the Coordinator for Counterterrorism to help address some of the security concerns and political sensitivities associated with conducting such assessments. We have previously reported on DOD efforts to coordinate with the Department of State on similar sensitive matters involving foreign governments' support for DOD assets abroad. For example, we have previously reported that through the Department of State, the United States and host-nation governments have successfully established various types of agreements—including general agreements, intelligence exchange agreements, written agreements, and informal agreements—that have been used to help protect U.S. forces and facilities abroad,[46] and nothing prohibits DOD from developing a similar approach for conducting DCIP vulnerability assessments on non-DOD-owned most critical assets in foreign countries. Until DOD completes the vulnerability assessments on such assets, which DOD is also required to complete by October 2011, DOD officials will not know the extent of those assets' vulnerabilities to electrical power disruptions.

[46] GAO, *Combating Terrorism: Improved Training and Guidance Needed to More Effectively Address Host Nation Support and Enhance DOD's Force Protection Efforts*, GAO-07-200NI (Washington, D.C.: Jan. 31, 2007).

The Defense Infrastructure Sector Lead Agent for Public Works Has Not Completed Its Technical Analysis of Public Works Infrastructure (Including Electricity) Supporting DOD Critical Assets

The U.S. Army Corps of Engineers (Corps)—which serves as DCIP's DISLA for Public Works (including electricity)—has not completed preliminary technical analyses of DOD installation infrastructure. Such analyses are intended to identify public works infrastructure networks, assets, points of service, and inter- and intradependencies that support the critical assets on DOD installations.[47] ASD(HD&ASA) requested these analyses for all the most critical assets from the Corps in order to support the teams conducting DCIP vulnerability assessments on those assets. Preliminary desktop analyses are intended to help brief DCIP vulnerability assessment teams on the most critical assets' supporting public works infrastructure—including electrical power systems—before those teams conduct the vulnerability assessments on the assets in the field.[48] According to ASD(HD&ASA), the Corps has completed these analyses for public works infrastructure located outside of DOD installations with the most critical assets. However, as of July 2009, the Corps had not yet conducted these analyses for public works infrastructure located within DOD installations for any of the most critical assets. According to a Corps official, the Corps has been unable to begin these analyses because it has not received infrastructure-related information that it requires from the military services.[49] According to the official, the Corps has been requesting this infrastructure-related information informally from the military services for several months and recently augmented its requests with formal written requests to the services. However, as of July 2009, the U.S. Navy is the only service that has begun to gather the requested information. In written correspondence with us, the remaining two military departments have indicated that limited funds and personnel will affect their ability to respond to the Corps' request for the infrastructure-

[47] We have previously reported on delays in the completion of important sector-specific interdependency analyses by the various DCIP Defense Infrastructure Sector Lead Agents. See GAO, *Defense Infrastructure: Actions Needed to Guide DOD's Efforts to Identify, Prioritize, and Assess Its Critical Infrastructure*, GAO-07-461 (Washington, D.C.: May 24, 2007).

[48] ASD(HD&ASA) also has requested that the Mission Assurance Division of the Naval Surface Warfare Center at Dahlgren, Virginia, support the DCIP vulnerability assessments by conducting similar desktop technical analyses of the commercial public works infrastructure that supports DOD's most critical assets outside of DOD installations. The Mission Assurance Division has completed these assessments for all DOD's most critical assets.

[49] The information requested includes Geographic Information System spatial data and imagery of installations' electrical systems, including data about the systems' size and capacity, power plants, transmission lines, substations, distribution lines, and emergency generators.

related information, which one of the services considers to be an unfunded mandate. Without this information, however, the Corps will be unable to conduct its preliminary technical analyses of public works infrastructure, including electrical power systems, which support the most critical assets. As a result, the teams conducting DCIP vulnerability assessments will be unable to consider crucial background information about the most critical assets' public works infrastructure—including networks, assets, points of service, and inter- and intradependencies related to electrical power systems—before the teams conduct the DCIP vulnerability assessments in the field.

DCIP Vulnerability Assessments Are Not Systematically Coordinated with Those from Related Mission Assurance Programs

DOD does not systematically coordinate DCIP vulnerability assessment policy, guidelines, or processes with those of other, related DOD mission-assurance programs that also examine electrical power vulnerabilities of DOD critical assets. DOD Directive 3020.40 calls for DCIP to complement other DOD mission assurance programs and efforts, including force protection; antiterrorism; information assurance; continuity of operations; chemical, biological, radiological, nuclear, and high-explosive defense; readiness; and installation preparedness. Vulnerability assessments from these other mission programs and efforts also examine electrical power vulnerabilities of DOD critical assets. For example, as part of DOD's antiterrorism and force protection efforts, the Defense Threat Reduction Agency conducts Joint Staff Integrated Vulnerability Assessments at selected DOD installations worldwide, including some that host critical assets. These assessments identify vulnerabilities related to terrorism and force protection at the selected installations, including those related to electrical power systems, and provide options to assist installation commanders in mitigating or overcoming the vulnerabilities. Similarly, as part of the critical asset protection processes, the military services also conduct vulnerability assessments related to mission assurance at installations that may also host critical assets. However, DOD Directive 3020.40 does not provide specific guidelines or requirements for systematically coordinating policy, guidelines, and processes or the results from DCIP vulnerability assessments on the critical assets with those of other DOD mission assurance programs.

ASD(HD&ASA) and Joint Staff officials acknowledge the benefits of coordinating and leveraging the results of assessments from DCIP and other DOD mission assurance programs—particularly those related to antiterrorism/force protection, continuity of operations, and information assurance—and have already taken some steps to further such coordination. For example, as of June 2009, the Defense Threat Reduction

Agency has conducted DCIP vulnerability assessments on 12 of the most critical assets in conjunction with Joint Staff Integrated Vulnerability Assessments being conducted on installations that host those assets,[50] while the military services have conducted DCIP vulnerability assessments on 2 of the most critical assets. Also, according to ASD(HD&ASA) and Joint Staff officials, the results of other DOD mission assurance vulnerability assessments already conducted on critical assets are made available for DCIP vulnerability assessment teams to consider before they conduct the DCIP vulnerability assessments. In addition, the Joint Staff and the Defense Threat Reduction Agency have begun to develop a formal agreement to align more closely the standards and benchmarks used to conduct vulnerability assessments for related DOD mission assurance programs, particularly DCIP, antiterrorism/force protection, continuity of operations, and information assurance.[51] However, until DOD finalizes the guidelines being developed in this agreement, it may be unable to systematically leverage the results of related vulnerability assessments that may be conducted on the same critical assets by multiple sources, and thus enhance DOD's ability to identify those assets' electrical power vulnerabilities.

[50] During these combined assessments, a DCIP vulnerability assessment module using DCIP-specific assessment benchmarks is added to the Joint Staff Integrated Vulnerability Assessment, which is conducted using different assessment standards. According to ASD(HD&ASA) officials, conducting these two assessments simultaneously also decreases the negative impacts and disruptions to the installation's commands from the assessment team's visit.

[51] According to Joint Staff officials, the agreement may be finalized by calendar year 2011 but will first require the full transfer of all antiterrorism program elements from the previous DOD program of responsibility in the Office of the Assistant Secretary of Defense for Special Operations/Low Intensity Conflict and Interdependent Capabilities to the new program of responsibility in ASD(HD&ASA).

DCIP Assessments to Date Do Not Consistently Consider Vulnerabilities to Longer-Term Power Disruptions

DCIP vulnerability assessment teams do not consistently consider the vulnerabilities of the critical assets to longer-term electrical power disruptions on a mission-specific basis,[52] which is not explicitly defined in the DCIP vulnerability assessment benchmarks for electrical power. These benchmarks serve as detailed criteria by which DCIP vulnerability assessment teams assess whether the electrical power networks[53] that support the critical assets—at the host installation and in the supporting off-site electrical power system—have the "capacity, redundancy, path diversity, security, survivability, and reliability to properly support a given mission."[54] Although the benchmarks consider how long electrical power backup systems can sustain continuity of critical operations, how to define what an unacceptable loss of power is, and whether the asset owner maintains a contingency plan to ensure availability of the electrical power network to accomplish an asset's mission, they do not explicitly consider vulnerabilities related to longer-term electrical power disruptions. As a result, DOD's DCIP vulnerability assessments may only focus on vulnerabilities associated with shorter-term electrical power disruptions.

According to ASD(HD&ASA) officials, DCIP vulnerability assessment teams already consider longer-term electrical power disruptions indirectly through questions in the benchmarks that ask about contingency plans and continuity of operations. However, we found that the DCIP

[52] Definitions of "longer-term" or "extended" electrical power disruptions vary. See footnote 19 on page 7.

[53] The DCIP vulnerability assessment benchmarks for electrical power define an electrical power network as consisting of substations, transmission lines, and power plants, each of which contain equipment, including transformers, circuit breakers, switches, and supervisory control and data acquisition systems.

[54] The benchmarks consist of questions to determine whether the owner of a most critical asset is (1) maintaining information about the configuration of the electrical power system that directly supports the critical asset; (2) determining if the electrical power system has the ability to meet the current and identified electrical power needs of the asset; (3) identifying all system assets essential to supporting the continued and reliable delivery of electrical power to the asset; (4) maintaining security to protect against threats and hazards to all identified critical electrical power assets, including identifying the network's single points of failure, if applicable (for commercial assets, DOD may work with the owner of the electrical power equipment and installations to enhance equipment security on a case-by-case basis); (5) maintaining mitigation options and plans to eliminate or reduce the potential impact to a mission in the event of an electrical system disruption with appropriate government and commercial electrical power suppliers and on-site operators/maintainers (e.g., backup generators, uninterruptible power supplies, and redundant feeds); (6) conducting routine preventive maintenance and testing of electrical power system components; and (7) identifying dependencies on and support provided to other supporting infrastructure to the asset.

vulnerability assessment reports that were available for 10 of the 34 most critical assets did not explicitly consider specific vulnerabilities or risk mitigation options associated with longer-term electrical power disruptions on a mission-specific basis. Consequently, such vulnerabilities or options may not be identified and DOD may not make appropriate risk management decisions.

Nevertheless, several DOD sources have recognized the need for the department to more explicitly consider the effects of longer-term electrical power disruptions to DOD's critical assets. For example, the Department of *Defense Energy Manager's Handbook*[55] calls for DOD components to develop strategies for both short- and long-term energy disruptions, including electricity disruptions. Also, in its February 2008 report, the Defense Science Board Task Force on DOD Energy Strategy—which concluded that DOD's critical national security and homeland defense missions were at an unacceptably high risk of failure from extended power disruptions—recommended that DOD consider the duration of electrical power disruptions, among other factors, in its risk management approach to reducing risks to critical missions from the loss of commercial electrical power. An update by the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics on DOD's Energy Security Task Force also proposed a subgoal of "reduc[ing] the risk of loss of critical functions due to extended commercial grid power disruptions at fixed installations." Without explicit guidance in the DCIP vulnerability assessment benchmarks for considering longer-term electrical power disruptions, future DCIP vulnerability assessments on other critical assets may be unable to identify vulnerabilities associated specifically with such electrical power disruptions.

[55] Office of the Deputy Under Secretary of Defense for Installations and Environment, *Department of Defense Energy Manager's Handbook* (Washington, D.C., Aug. 25, 2005).

DOD Has Taken Steps to Assure Availability of Electrical Power to Critical Assets, but It Lacks a Mechanism for Tracking Implementation, and Its Coordination with Electricity Providers Remains Limited

DOD Has Taken Some Steps to Assure the Availability of Electrical Power to Its Critical Assets

DOD has taken some steps to assure the availability of its electrical power supplies by identifying and addressing the vulnerabilities and risks of its critical assets to electrical power disruptions. For example, from August 2005 through October 2008, DOD issued Defense Critical Infrastructure Program guidance for identifying critical assets, assessing their vulnerabilities, and making risk management decisions about those vulnerabilities. Also, as previously discussed, DOD has conducted DCIP vulnerability assessments on 14 of the 34 most critical assets and has scheduled assessments for 13 of the remaining assets, but it has not yet scheduled assessments for 5 of the non-DOD-owned most critical assets.[56] The DCIP vulnerability assessments conducted so far have identified specific electrical power–related vulnerabilities to some of the critical assets, including vulnerabilities associated with the reliability of the assets' supporting commercial electrical power grid, the availability of backup electrical power supplies, and single points of failure in electrical power systems supporting the assets.[57] Addressing the risks associated with these vulnerabilities—by remediating, mitigating, or accepting those risks—can

[56] DOD has also not yet scheduled DCIP vulnerability assessments for two DOD-owned most critical assets.

[57] We observed during our site visits to six of the most critical assets that all six assets depend on unsecured, overhead electrical power lines that constitute single points of failure. According to DOD officials at one of these sites, animals caused a disruption in the electrical power lines supporting one of these assets, resulting in mission failure.

help DOD assure the availability of electrical power to the critical assets. For example, at all 6 most critical assets we visited, the DOD asset owners have installed diesel-based electrical power generators as backup sources of electricity during electrical power disruptions. Other (non-DCIP) DOD mission assurance programs also have the potential to help DOD assure the availability of electrical power supplies to its most critical assets. For example, we found that Joint Service Integrated Vulnerability Assessments and similar vulnerability assessments from the military services, which have been conducted on some of the installations with critical assets for antiterrorism and force protection purposes, also have identified vulnerabilities related to electrical power.

Furthermore, DOD also has taken steps to coordinate with other federal agencies, including DOE and DHS, as well as electrical industry organizations, and these steps may help to assure the supply of electricity to its critical assets. For example, to represent its concerns and interests on electricity, DOD participates in the Energy Government Coordinating Council. The council provides DOD and other federal agencies with a forum for sharing their concerns, comments, and questions on energy-related matters—including critical infrastructure protection—with DOE, which chairs the group.[58] In another effort involving DOE, several DOD combatant commands—including U.S. European Command and U.S. Africa Command—have recently agreed to accept a DOE departmental representative to serve as an energy attaché to the commands. The DOE representatives will provide energy-related expertise to their respective commands, particularly with respect to the commands' energy-related planning activities and the security and reliability of the commands' energy infrastructure. DOD has also partnered with various federal agencies and industry organizations to further increase the assurance of electrical power. For example, DOD serves as co-chair of the federal Task Force on Electric Grid Vulnerability of the National Science and

[58] The Energy Government Coordinating Council is one of 18 governmental coordinating councils created within the framework of the *National Infrastructure Protection Plan*. Issued in June 2006, the plan serves as a road map for DHS and other relevant stakeholders, such as owners and operators of key critical infrastructure, to use risk management principles to prioritize protection activities within and across sectors in an integrated, coordinated fashion. Each sector is assigned a lead sector agent, with the Energy Sector and its Government Coordinating Council led by DOE. The purpose of this council is to create the structure through which respective groups from all levels of government and the private sector can participate in planning efforts related to the development of sector-specific plans and implement efforts to protect critical infrastructure, among other things.

Technology Council's Committee on Homeland and National Security, which was established in January 2009 to identify research and development needs for electrical grid vulnerabilities and to coordinate with other federal agencies to address those needs.[59] In addition, DOD officials are collaborating with a working group established by the Edison Electric Institute in early 2009 called the Energy Security Partnership Group. The group focuses on improving communications between DOD and its utilities and on identifying and removing barriers to the development of comprehensive energy security programs at DOD installations. Also, in July 2009, DOD participated in an interagency exercise cosponsored by DHS, DOE, and DOD called Secure Grid 2009, Electric Grid Tabletop Exercise, for which officials from DOD, DOE, DHS, the Federal Energy Regulatory Commission, the North American Electric Reliability Corporation, and the Edison Electric Institute, among others, jointly developed recommendations and potential responses to two scenarios involving theoretical physical and cyber-related attacks on U.S. electrical power grids.

Our survey results confirm that some steps are being taken at various levels within DOD to improve the assurance of electrical power supplies to its most critical assets. For example, according to the survey and reports we reviewed, DOD conducted vulnerability and risk assessments involving electrical power on 24 of the most critical assets through a variety of DOD mission assurance reviews, including DCIP assessments, Joint Staff Integrated Vulnerability Assessments, combatant command assessments, DOD agency assessments, and local installation assessments. The survey results also indicate that secondary sources of electricity—such as uninterruptible power supply systems and diesel generators—provide some backup electrical power capabilities to almost all of the critical assets. In addition, according to the survey, asset owners and host installations for some of the critical assets whose vulnerabilities have been assessed have taken specific measures to address those vulnerabilities, such as eliminating single points of failure, developing electrical power disruption contingency plans, installing emergency electrical power generators, and increasing physical security measures around electrical power facilities.

[59] Members of the Task Force on Electric Grid Vulnerability represent DOD (Co-Chair), DOE (Co-Chair), DHS, the Director of National Intelligence, the Environmental Protection Agency, the Federal Energy Regulatory Commission, the National Aeronautics and Space Administration, the Nuclear Regulatory Commission, the Office of Science and Technology Policy, and the Office of Management and Budget.

DOD Lacks a Mechanism for Tracking Implementation of Future DCIP Risk Management Decisions and Responses to Vulnerabilities

DOD has not yet established a mechanism for systematically tracking the implementation of future DCIP risk management decisions, which are intended to address vulnerabilities (including those involving electrical power) that have been identified for the most critical assets. Such tracking could help DOD ensure that DCIP stakeholders are developing and implementing measures to address the most critical assets' identified vulnerabilities to electrical power disruptions and thereby help assure the availability of electrical power to those assets.[60] As previously discussed, DCIP's risk management program involves the identification of DOD's most critical assets; the assessment of those assets' vulnerabilities through vulnerability assessments; and subsequent risk assessments, risk management decisions, and risk responses involving relevant DCIP stakeholders. DCIP guidance contained in DOD Instruction 3020.45 requires stakeholders to coordinate to make risk management decisions regarding whether and how to address identified vulnerabilities—through remediation or mitigation—or accept the risk posed by not addressing those vulnerabilities.[61]

Under DCIP, ASD(HD&ASA) has overall responsibility for overseeing the implementation of actions for the remediation, mitigation, or acceptance of risks to DOD critical assets, while owners of the critical assets are required to monitor the status and progress of the implementation of DCIP risk management decisions for their respective assets.[62] ASD(HD&ASA) officials indicated to us that they do not systematically track the results of DCIP vulnerability assessments, asserting that they consider it more important to track the implementation of the subsequent DCIP risk management decisions and responses to be made concerning the vulnerabilities that are identified. The officials told us that these risk management decisions would reflect the consensus that would be reached

[60] The Government Performance and Results Act encourages government agencies to establish performance indicators to be used in measuring or assessing the relevant outputs, service levels, and outcomes of each program activity. The implementation of DCIP risk management decisions could serve as one performance indicator of the extent to which DCIP activities are reducing vulnerabilities (including those related to electrical power) of DOD's most critical assets.

[61] Remediation actions are those steps taken to correct known deficiencies and weaknesses once a vulnerability has been identified. Mitigation actions are those taken in response to a warning or after an incident occurs to lessen the potentially adverse effects on a given military operation or infrastructure.

[62] DOD Instruction 3020.45, *Defense Critical Infrastructure Program (DCIP) Management*, sections 5.1 and E3.2.3.3.

by relevant DCIP stakeholders (such as asset owners, mission owners, and defense infrastructure sector lead agents) on either remediating, mitigating, or accepting specific vulnerabilities—actions that may require the stakeholders to provide funding or other resources in order to implement.[63] However, the officials have not yet tracked any such decisions or responses, because no such decisions or responses have yet been made in response to the 14 DCIP vulnerability assessments conducted so far. According to these officials, because of the number of stakeholders and potential resources involved, risk management decisions can take several months to coordinate following a DCIP vulnerability assessment. These officials said that they plan to monitor the implementation of DCIP risk management decisions and responses, but they have not yet developed a mechanism, such as a schedule to track the implementation status of those decisions and responses, by which to do so. Without systematic tracking of risk management decisions and responses, DOD may be unable to comprehensively determine whether asset owners and host installations are taking the steps agreed to by relevant DCIP stakeholders to address the vulnerabilities of the critical assets, including vulnerabilities related to electrical power disruptions.

DOD's Coordination with Local Electricity Providers Has Been Limited

DCIP guidance recognizes the importance of collaboration by encouraging coordination[64] between DOD facilities with critical assets and their respective public utilities—including electricity providers—in order to remediate risks involving those utilities.[65] According to this guidance, a DOD installation "should establish good communications with public service providers [including electrical power providers] about service requirements," and "that relationship does not have to wait for the identification of a vulnerability," as "the remediation of risks posed by commercial dependency may be more complicated than that of DOD-

[63] After a DCIP vulnerability assessment on a most critical asset, the owner of that asset conducts a corresponding risk assessment for the most critical asset and shares it with other relevant DCIP stakeholders. Subsequently, relevant DCIP stakeholders review the results of each risk assessment and jointly produce a "risk decision package" to formally document the risk management decisions and responses (i.e., remediation, mitigation, and risk acceptance measures) reached for each most critical asset.

[64] Coordination with local electricity providers may range from an informal working relationship with utility officials to a formal memorandum of agreement between the most critical asset's host installation and the electricity provider.

[65] DOD Manual 3020.45, Volume 2, *Defense Critical Infrastructure Program (DCIP): DCIP Remediation Planning* (Oct. 28, 2006).

owned infrastructure."[66] Similarly, in recognition of the important role that local utility providers play in supporting DOD installations with critical assets, the U.S. Army Corps of Engineers is requesting funds for a pilot program that would involve extensive collaboration with the local electricity providers at selected U.S. Army installations with critical assets. The pilot program is intended to analyze the reliability of community infrastructure in meeting current and anticipated needs of the installations and the critical missions.[67]

As previously discussed, our survey indicated that 31 of the DOD's 34 most critical assets identified the commercial electrical power grid as their primary source of electrical power. Yet despite this overwhelming reliance, host installations or owners of only 7 of the surveyed critical assets reported coordinating with their local electricity providers to either identify or address their assets' vulnerabilities to electrical power disruptions.[68] Furthermore, according to the survey and our analysis, none of the host installations or owners of the critical assets have developed any formal agreements with their local electricity providers to help manage the risks and vulnerabilities of those assets to electrical power disruptions. Survey respondents cited various reasons for not coordinating with local electricity providers, including the absence of a requirement for such coordination and the lack of a vulnerability assessment on the asset that would indicate the need to initiate such coordination.

Coordinating with local electricity providers could usefully enhance DOD's efforts to identify or address the vulnerabilities of critical assets to electrical power disruptions and thereby better assure the availability of electrical power to those assets. However, few host installations or owners of critical assets have coordinated with their local electrical power providers to help identify or address the assets' vulnerabilities to electrical power disruptions. According to an electrical power industry association representative, local electricity providers may have technical expertise or be pursuing activities that could help DOD installations develop risk remediation or mitigation measures to address electrical power

[66] DOD Manual 3020.45, Volume 2.

[67] The U.S. Army Corps of Engineers has named the pilot program the Community Resilience Proposal for DCIP Public Works Infrastructure.

[68] DOD officials at all six of the most critical assets we visited also told us that they did not know whether their local commercial electricity providers may have conducted their own vulnerability or risk assessments of the electrical power grids supporting those assets.

vulnerabilities affecting a critical asset.[69] According to this representative, such coordination, for example, could lead to agreements in which local electricity providers would prioritize the restoration of electrical power to a DOD installation with a critical asset following an electrical power disruption. In addition, DOD installations could usefully coordinate with their respective electricity providers concerning an industry initiative called Spare Transformer Equipment Program, in which electricity providers agree to share spare electrical power transformers—which are often foreign made, expensive, and can take several years to order—in the event of an emergency.[70] Without more extensive coordination between DOD DCIP stakeholders and local electricity providers, DOD may be limiting the risk remediation or mitigation options that it could consider for addressing the vulnerabilities of its critical assets to electrical power disruptions.

Conclusions

DOD relies on commercial electrical power grids for secure, uninterrupted electrical power supplies to support its most critical assets—those whose incapacitation or destruction would have a very serious, debilitating effect on the department's ability to fulfill its missions. However, according to the Defense Science Board Task Force on DOD Energy Strategy, the commercial electrical power grids have become increasingly fragile and vulnerable to extended power disruptions that could severely impact DOD's most critical assets, their supporting infrastructure, and the missions they support, and disruptions to the electrical power grid have occurred. DOD's most critical assets are vulnerable to disruptions in electrical power supplies, but DOD would benefit from additional

[69] According to the Edison Electrical Institute, for example, many electrical power utilities are implementing aggressive energy efficiency, demand response, smart grid, and renewable energy programs that may provide additional expertise and financial assistance to a local DOD installation's energy security program.

[70] The Federal Energy Regulatory Commission approved the Spare Transformer Equipment Program in September 2006. The program, an initiative of the Edison Electric Institute, represents a coordinated approach to increasing the utility industry's inventory of spare transformers and streamlining the process of transferring those transformers to affected utilities in the event of a transmission outage caused by a terrorist attack. Under the program, each participating utility is required to maintain and, if necessary, acquire a specific number of transformers. The program requires each participating utility to sell its spare transformers to any other participating utility that suffers a "triggering event," defined as an act of terrorism that destroys or disables one or more substations and results in a declared state of emergency by the President. Any investor-owned, government-owned, or rural electric cooperative utility in the United States or Canada may participate in the program.

information to determine the full extent of the risks and vulnerabilities these assets face. By completing DCIP vulnerability assessments on all of its most critical assets, DOD would have more information to determine the full extent of these assets' risks and vulnerabilities to such disruptions. Similarly, with additional guidelines, an implementation plan, and a schedule for conducting DCIP vulnerability assessments on all non-DOD-owned most critical assets, particularly those located abroad, DOD could more accurately determine the full extent of those assets' risks and vulnerabilities to such disruptions. Further, until the U.S. Army Corps of Engineers is able to complete the preliminary technical analyses of public works (including electrical power) infrastructure in support of the DCIP vulnerability assessments of the critical assets, DOD may be unable to identify all electrical power vulnerabilities to its most critical assets. Additionally, once DOD finalizes guidelines specifying how DCIP assessment criteria and processes should be coordinated with those of other DOD mission assurance programs, DOD could more systematically determine whether these programs may also be identifying electrical power vulnerabilities and risk management options for its most critical assets. Also, explicit guidelines to assess vulnerabilities to critical assets from long-term electrical power disruptions would further enhance DOD's ability to manage the risks associated with such disruptions.

While DOD has taken some steps toward assuring the availability of its electrical power supplies to its critical assets, additional DCIP measures could further enhance efforts to address these assets' risks and vulnerabilities to electrical power disturbances. DOD could also improve its ability to leverage related mission assurance assessments and respond to future disruptions by developing a mechanism to systematically track the results of future risk management decisions and responses intended to address risks and vulnerabilities identified for the most critical assets. Additionally, DOD could expand its options for addressing disruptions in the commercial electrical power grid by encouraging greater collaboration between the owners or host installations of the most critical assets and their respective local electricity providers.

With more comprehensive knowledge of DOD's most critical assets' risks and vulnerabilities to electrical power disruptions and more effective coordination with electricity providers, DOD can better avoid compromising crucial DOD-wide missions during electrical power disruptions. This additional information may also improve DOD's ability to effectively prioritize funding needed to address identified risks and vulnerabilities of its most critical assets to electrical power disruptions.

Recommendations for Executive Action

To ensure that DOD has sufficient information to determine the full extent of the risks and vulnerabilities to electrical power disruptions of its most critical assets, we recommend that the Secretary of Defense direct the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs, in collaboration with the Joint Staff's Directorate for Antiterrorism and Homeland Defense, combatant commands, military services, and other Defense Critical Infrastructure Program stakeholders, as appropriate, to take the following five actions:

- Complete Defense Critical Infrastructure Program vulnerability assessments, as required by DOD Instruction 3020.45, on all of DOD's most critical assets by October 2011.
- Develop additional guidelines, an implementation plan, and a schedule for conducting Defense Critical Infrastructure Program vulnerability assessments on all non-DOD-owned most critical assets located in the United States and abroad in conjunction with other federal agencies, as appropriate, that have a capability to implement the plan.
- Establish a time frame for the military services to provide the infrastructure data required for the Public Works Defense Infrastructure Sector Lead Agent—the U.S. Army Corps of Engineers—to complete its preliminary technical analysis of public works (including electrical system) infrastructure at DOD installations that support DOD's most critical assets.
- Finalize guidelines currently being developed to coordinate Defense Critical Infrastructure Program assessment criteria and processes more systematically with those of other DOD mission assurance programs.
- Develop explicit Defense Critical Infrastructure Program guidelines for assessing the critical assets' vulnerabilities to long-term electrical power disruptions.

To enhance DOD's efforts to mitigate these assets' risks and vulnerabilities to electrical power disruptions and leverage previous assessments and multiple asset owners' information, we recommend that the Secretary of Defense direct the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs, in collaboration with the Joint Staff's Directorate for Antiterrorism and Homeland Defense, combatant commands, military services, and other Defense Critical Infrastructure Program stakeholders, as appropriate, to take the following two actions:

- Develop a mechanism to systematically track the implementation of future Defense Critical Infrastructure Program risk management decisions and responses intended to address electrical power–related risks and vulnerabilities to DOD's most critical assets.

- Ensure for DOD-owned most critical assets, and facilitate for non-DOD-owned most critical assets, that asset owners or host installations of the most critical assets, where appropriate, reach out to local electricity providers in an effort to coordinate and help remediate or mitigate risks and vulnerabilities to electrical power disruptions that may be identified for DOD's most critical assets.

Agency Comments and Our Evaluation

In written comments on a draft of this report, DOD concurred with all of our recommendations and provided technical comments, which we incorporated in the report where appropriate.[71] DOD's comments are reprinted in appendix VI. Due to the sensitivity of DOD's most critical assets and its concerns about the classification and dissemination of the initial draft report, as well as the focus of the recommendations on DOD's program, we did not request agency comments on the full draft report from DOE, DHS, and the Federal Energy Regulatory Commission. However, we did seek technical comments from these entities on sections of the initial draft report that pertained to their roles and responsibilities, which we also incorporated in the report where appropriate.

DOD concurred with our five recommendations to ensure that DOD has sufficient information to determine the full extent of the risks and vulnerabilities to electrical power disruptions of its most critical assets. Based on DOD's comments, we modified our original recommendation concerning the establishment of a time frame for the military services to provide the infrastructure data required for preliminary technical analysis of public works (including electrical system) infrastructure at DOD installations that support DOD's most critical assets.

- First, DOD concurred with our recommendation that the department complete DCIP vulnerability assessments on all of its most critical assets by October 2011, as required by DOD Instruction 3020.45. DOD noted that the Joint Staff, in coordination with ASD(HD&ASA), has already begun to conduct these assessments using an all-hazards and mission-assurance approach. As we reported, as of June 2009, DOD had conducted DCIP assessments on 14 of the 34 most critical assets.

[71] The cover letter for DOD's written comments indicates that the DOD Office of Security Review reviewed the draft report and recommended that the draft report be protected at the SECRET level. However, by deleting certain sections from the draft report, we were able to issue this unclassified report with the approval of the DOD Office of Security Review with a different report number.

- Second, DOD concurred with our recommendation that the department develop additional guidelines, an implementation plan, and a schedule for conducting vulnerability assessments on all non-DOD-owned most critical assets located in the United States and abroad in conjunction with other federal agencies, as appropriate, that have a capability to implement the plan. DOD acknowledged that conducting vulnerability assessments on such assets, particularly those located abroad, presents significant challenges, as they require the agreement of the assets' non-DOD owners. According to the department, the ASD(HD&ASA)/DCIP Office is coordinating with appropriate offices to examine the possibility of conducting "remote assessments" on these assets. We recognize the challenges faced by DOD in identifying the electrical power vulnerabilities of non-DOD-owned critical assets and support DOD's efforts to coordinate with appropriate federal agencies in this area. We previously have reported on DOD's efforts to coordinate with the Department of State on similar sensitive matters involving foreign governments' support for DOD assets abroad, noting that such efforts have resulted in various types of agreements to help protect U.S. forces and facilities abroad. We also note that if DOD decides to conduct "remote" DCIP vulnerability assessments on the non-DOD-owned most critical assets, such assessments should rely on the same benchmarks used for conducting DCIP vulnerability assessments on DOD-owned most critical assets.
- Third, DOD concurred with our recommendation that the department establish a time frame for the military services to provide the infrastructure data required for the Public Works Infrastructure Sector Lead Agent—the U.S. Army Corps of Engineers—to complete its preliminary technical analysis of public works infrastructure at DOD installations that support DOD's most critical assets. Based on comments from DOD that the Corps has already completed the technical analysis for public works infrastructure located outside of the installations, but is still waiting for the data required to complete the analysis on infrastructure located within the installations, we modified this recommendation to indicate that these data are required for completing—rather than conducting—the preliminary technical analysis. DOD acknowledged that such information is necessary for the proper characterization of its critical assets from a public works perspective. We believe that the establishment of specific time frames for the military services to provide this important information is necessary because, as of July 2009, only one of the military services—the U.S. Navy—had begun to gather the requested information.
- Fourth, DOD concurred with our recommendation that the department finalize guidelines currently being developed to coordinate DCIP assessment criteria and processes more systematically with those of

other DOD mission-assurance programs. While acknowledging the synergistic effect of complementary risk management program activities and security-related functions, DOD noted that such programs are subject to different directives and appropriations, and that critical infrastructure protection at the installation level is not yet mature. According to DOD, the Joint Staff is now overseeing a "way ahead" process to better synchronize these efforts. We encourage the Joint Staff to complete this initiative and identify specific ways for coordinating DCIP assessment criteria and processes more systematically with those of DOD's other mission assurance programs.

- Fifth, DOD concurred with our recommendation that the department develop explicit DCIP guidelines for assessing the most critical assets' risks and vulnerabilities to long-term electrical power disruptions. According to DOD, the ASD(HD&ASA)/DCIP Office will review current vulnerability assessment criteria and standards and work with the Joint Staff to include considerations of long-term electrical power disruptions.

DOD also concurred with our two recommendations to enhance DOD's efforts to mitigate its most critical assets' risks and vulnerabilities to electrical power disruptions and leverage previous assessments and multiple asset owners' information:

- First, DOD concurred with our recommendation that the department develop a mechanism to systematically track the implementation of future DCIP risk management decisions and responses intended to address electrical power–related risks and vulnerabilities to DOD's most critical assets. According to DOD, the ASD(HD&ASA)/DCIP Office has developed draft DOD Manual 3020.45, Volume 5, *Defense Critical Infrastructure Program (DCIP) Coordination Timeline*, that is being coordinated within the department. DOD notes that manual's purpose is to provide uniform procedures and timelines for DCIP stakeholders—that is, ASD(HD&ASA), the Joint Staff, military departments, combatant commands, defense agencies, and DISLAs—to execute DCIP activities and responsibilities, including those related to risk management decisions and responses. We encourage DOD to finalize this draft manual and ensure that it provides explicit guidance on tracking the implementation of DCIP risk management decisions and responses resulting from DCIP vulnerability assessments of DOD's most critical assets. DOD also notes that the DCIP Office is developing an automated Critical Asset Identification Process Collaboration Tool that will document and track the status of DCIP stakeholders' progress in the DCIP risk management process.
- Second, DOD also concurred with our recommendation that the department ensure for DOD-owned most critical assets, and facilitate

for non-DOD-owned most critical assets, that asset owners or host installations of the most critical assets, where appropriate, reach out to local electricity providers in an effort to coordinate and help remediate or mitigate risks and vulnerabilities to electrical power disruptions that may be identified for DOD's most critical assets. DOD's comments cited existing guidance that, among other things, (1) encourages government and private-sector decision makers to work with electricity providers to identify remedies to potential single points of failure and (2) advises DOD facility managers to establish good communications with public service providers about service requirements, and to review service-level agreements, acquisition programs, contracts, and operational processes for opportunities to address and include stronger resiliency language and requirements for future remediation efforts. According to DOD, this guidance will be reinforced at DCIP forums for collaboration, such as meetings of the Defense Critical Infrastructure Integration Staff, Operational Advisory Board, and Defense Infrastructure Sector Council. We encourage DOD to reinforce such guidance concerning collaboration with local electricity providers directly with asset owners or host installations for each of the most critical assets, as appropriate, in order to help mitigate the risks and vulnerabilities to electrical power disruptions that may be identified for those assets.

We are sending copies of this report to other interested congressional parties; the Secretary of Defense; the Chairman, Joint Chiefs of Staff; the Secretaries of the U.S. Army, the U.S. Navy, and the U.S. Air Force; the Commandant of the U.S. Marine Corps; and the Director, Office of Management and Budget. This report also is available at no charge on GAO's Web site at http://www.gao.gov.

If you or your staff have any questions concerning this report, please contact me at (202) 512-5431 or dagostinod@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix VII.

Davi M. D'Agostino
Director
Defense Capabilities and Management

List of Committees

The Honorable Carl Levin
Chairman
The Honorable John McCain
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Daniel K. Inouye
Chairman
The Honorable Thad Cochran
Ranking Member
Subcommittee on Defense
Committee on Appropriations
United States Senate

The Honorable Tim Johnson
Chairman
The Honorable Kay Bailey Hutchison
Ranking Member
Subcommittee on Military Construction,
Veterans Affairs, and Related Agencies
Committee on Appropriations
United States Senate

The Honorable Ike Skelton
Chairman
The Honorable Howard P. McKeon
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable John P. Murtha
Chairman
The Honorable C.W. Bill Young
Ranking Member
Subcommittee on Defense
Committee on Appropriations
House of Representatives

The Honorable Chet Edwards
Chair
The Honorable Zach Wamp
Ranking Member
Subcommittee on Military Construction,
Veterans Affairs, and Related Agencies
Committee on Appropriations
House of Representatives

Appendix I: Scope and Methodology

To conduct our review of the assurance of electrical power supplies to Department of Defense (DOD) critical assets, we administered three structured written surveys to the owners or those with program responsibility for 100 percent of DOD's 34 most critical assets, which DOD identified through the Defense Critical Infrastructure Program (DCIP) as its most critical assets as of October 2008. We administered one survey to the military services and DOD agencies that own or have program responsibility for the assets through DCIP to obtain information about the (1) assets' degree of reliance on electrical power; (2) assets' primary and backup sources of electrical power supplies; (3) number and type of unplanned electrical power disruptions to the assets; (4) DCIP and non-DCIP assessments of the assets' risks and vulnerabilities to electrical power disruptions from January 2006 through December 2008; and (5) measures recommended, implemented, or planned to address or manage such risks and vulnerabilities. We administered another survey to the Joint Staff to obtain information about the missions supported by the assets. Finally, we administered the third survey to the Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD(HD&ASA)) regarding coordination efforts with relevant DOD and non-DOD stakeholders. (These surveys are reproduced in full in apps. III, IV, and V, respectively.) We limited our surveys to the universe of DOD's most critical assets because of concerns over the reliability of DOD's larger list of about 675 Tier 1 Task Critical Assets,[1] which support critical DOD missions at the departmental, combatant command, and military service levels. We also conducted six follow-up site visits to a nonprobability sample of critical assets to verify and validate the surveys' results and evaluate in-depth issues identified in the surveys' responses. We selected the sites for visits judgmentally based on the survey responses regarding issues addressed in this report.

We initially selected a random sample from DOD's universe of about 675 Tier 1 Task Critical Assets to survey for this review. However, based on discussions with DOD officials and our own analysis, we found significant data reliability and validity problems with DOD's Tier 1 Task Critical Asset list. We found that the use of disparate sets of guidance, including draft and nonbinding guidance, resulted in the selection and submission of assets to the Tier 1 Task Critical Asset list based on inconsistent criteria,

[1] A Tier 1 Task Critical Asset is an asset the loss, incapacitation, or disruption of which could result in mission (or function) failure at the DOD, military department, combatant command, subunified command, defense agency, or defense infrastructure sector level.

thus limiting the usefulness of the Tier 1 Task Critical Asset list to DOD decision makers in determining DOD's most critical assets and prioritizing funding to address identified vulnerabilities. As a result, we determined that for methodological purposes, DOD's current Tier 1 Task Critical Asset list did not represent a meaningful universe from which we should select our survey sample or to which we should project our survey results. Because the universe of critical assets did not represent an accurate, comprehensive list of DOD Tier 1 Task Critical Assets, we determined that this issue in and of itself warranted further analysis. Therefore, we issued a separate report,[2] with recommendations, on issues relating specifically to the Tier 1 Task Critical Asset list to enable DOD to take timely actions to update and improve its list of Defense Critical Assets in the fall of 2009 and prioritize funding.

In addition to our survey, we obtained relevant documentation and interviewed officials from the following DOD organizations:

- Office of the Deputy Under Secretary of Defense for Installations and Environment
- ASD(HD&ASA)/DCIP Office
- Joint Staff (J-34), Directorate for Antiterrorism/Homeland Defense, DCIP Resources and Assessments Branch
- Military Services
  - Headquarters, Department of the Army
    - Critical Infrastructure Risk Management Branch
    - Headquarters, Installation Management Command, Anti-Terrorism/Force Protection
    - Office of the Assistant Chief of Staff for Installation Management, Energy & Utilities for Installation Office
  - Headquarters, Department of the Navy
    - Critical Infrastructure Protection
  - Headquarters, U.S. Marine Corps
    - Marine Corps Critical Infrastructure Program, Mission Assurance Branch
  - Headquarters, Department of the Air Force
    - Assistant Deputy Chief of Staff Logistics, Installations, and Mission Support
    - Critical Infrastructure Program, Air Force Directorate of Current Operations & Training, Air Force Homeland Defense Division
- Defense Information Systems Agency

[2] GAO-09-740R.

- Defense Infrastructure Sector Lead Agents
  - Headquarters, U.S. Army Corps of Engineers, DCIP Public Works Defense Sector Lead
- Defense Threat Reduction Agency, Support Branch Chief, Combat Support Assessments Division
- Director of Defense Research and Engineering
- Defense Science Board, Task Force on DOD Energy Strategy
- Mission Assurance Division, Naval Surface Warfare Center at Dahlgren
- Selected DOD critical assets at U.S. military installations within the continental United States

To become more familiar with efforts currently taking place to assure the nation's electrical power grid, we met with various officials from federal agencies, electrical power industry associations, and private-sector entities and other officials to determine their roles and responsibilities, ongoing initiatives, and the extent of their coordination efforts with DOD in assuring electrical power to the nation's power grid. We obtained relevant documentation and interviewed officials from the following organizations:

- Department of Homeland Security (DHS)
  - National Protection and Programs Directorate
  - Office of Infrastructure Protection
  - Infrastructure Information Collection Division
  - Partnership and Outreach Division
  - Protective Security Coordination Division
  - Office of Cybersecurity and Communications
- Department of Energy (DOE), Office of Electricity Delivery & Energy Reliability
- Federal Energy Regulatory Commission, Office of Electric Reliability
- North American Electric Reliability Corporation
- CACI International, Inc.
- Edison Electric Institute
- Pareto Energy, Inc.
- Talisman International, LLC

We did not request agency comments from DOE, DHS, and the Federal Energy Regulatory Commission on the full draft report, which at the time was classified as SECRET because of (1) DOD's concerns about the classification and dissemination of the report and (2) the focus of the recommendations on DOD's program. We did seek technical comments from these entities on sections of the initial draft report that pertained to their roles and responsibilities, which we incorporated in the report where appropriate. We also shared sections of the initial draft report that discussed the 2008 *Report of the Defense Science Board Task Force on*

DOD Energy Strategy, "More Fight—Less Fuel," and the entities either agreed or did not take issue with the conclusions of this report.

To learn more about the assurance of electrical power supplies to DOD critical assets, we developed three electronic surveys for DOD critical assets, their missions, and coordination efforts regarding the assets. We asked responders about (1) missions supported by the assets; (2) assets' degree of reliance on electrical power; (3) assets' primary and backup sources of electrical power supplies; (4) number and type of unplanned electrical power disruptions to the assets; (5) DCIP and non-DCIP assessments of the assets' risks and vulnerabilities to electrical power disruptions; and (6) measures recommended, implemented, or planned to address or manage such risks and vulnerabilities, including coordination efforts with relevant DOD and non-DOD stakeholders.

We conducted our surveys from May 2009 through August 2009, using self-administered electronic surveys. We sent a questionnaire on DOD critical assets to the owners and operators of DOD-owned critical assets. We sent a second questionnaire on DOD critical asset missions to the Joint Staff (J-34). We sent a third questionnaire on coordination efforts for DOD critical assets to ASD(HD&ASA)/DCIP Office. We sent the questionnaires by SIPRNet in an attached Microsoft Word form that respondents could return electronically via SIPRNet after marking check boxes or entering responses up to the SECRET classification level into open answer boxes. We also made provisions for receiving completed questionnaires at the TOP SECRET classification level, if needed, via a GAO Joint Worldwide Intelligence Communications System account, which was established for us at the DOD Office of the Inspector General.

We sent the original three electronic questionnaires in May and June 2009. We sent out reminder e-mail messages at different times to all nonrespondents in order to encourage a higher response rate. In addition, we made several courtesy telephone calls to nonrespondents to encourage their completion of the surveys. All questionnaires were returned by August 2009. In the end, we achieved a 100 percent response rate.

Because this was not a sample survey, but rather a survey of the universe of respondents, it has no sampling errors. However, the practical difficulties of conducting any survey may introduce errors, commonly referred to as nonsampling errors. For example, difficulties in interpreting a particular question, determining sources of information available to respondents, or entering data into a database or analyzing them can introduce unwanted variability into the survey results. We took steps in

developing the questionnaire, collecting the data, and analyzing them to minimize such nonsampling error.

For example, design methodologists designed the questionnaire in collaboration with GAO staff who had subject matter expertise. In addition to an internal expert technical review by GAO's Survey Coordination Group, we pretested the survey with U.S. Army, U.S. Navy, and U.S. Air Force officials representing three most critical asset sites as well as officials from the Joint Staff (J-34) and ASD(HD&ASA) to ensure that the questions were relevant, clearly stated, and easy to understand. Since there were relatively few changes based on the pretests and because we were conducting surveys with the universe of respondents, we did not find it necessary to conduct additional pretests. Instead, changes to the content and format of the questionnaire were made after the pretests based on the feedback we received.

When we analyzed the data, an independent analyst checked all computer programs. All data were double keyed during the data entry process, and GAO staff traced and verified all of the resulting data to ensure accuracy.

To verify and validate the survey recipients' responses and evaluate in more detail issues identified in the surveys, we conducted six follow-up site visits to a nonprobability sample of surveyed assets. We selected the sites for visits judgmentally based on the survey responses regarding issues addressed in this report. During these site visits, we spoke with installation personnel, including asset owners and operators, about their reliance on supporting electrical infrastructure and electricity providers. While findings from our site visits are not generalizable to all 34 most critical assets, we obtained follow-up survey information from installation personnel for critical assets and visited those assets to validate the survey responses, as applicable. We clarified responders' interpretation of the survey questions, discussed their responses in detail, and visited the critical assets and their supporting infrastructure to better understand each asset's unique situation. Finally, we reviewed documentation and guidance related to those critical assets, including vulnerability assessments.

We conducted this performance audit from October 2008 through October 2009 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe

that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Typical Electrical Power Vulnerabilities and Remediation Measures

Common types of electrical power vulnerabilities	Examples of electrical power vulnerabilities	Possible remediation measures
Co-location of primary and backup electrical power equipment.	Both the primary and backup power supply systems exist in the same room for convenience of maintenance.	• Implement physical diversity in location of backup support. • Ensure fire suppression systems support continued operation of non-affected systems. • Increase security on the location during higher threat periods.
Single transformer provides both commercial and backup power to a critical asset.	Alternate paths that supply electrical power converge at single component (i.e., a transformer) and represent potential point of failure if common component fails.	• Have independent commercial and backup power paths. • Identify alternate location to relocate critical operations. • Use portable generations and uninterruptible power supplies to provide power in case of a single component failure. • Arrange for immediate emergency maintenance response to restore the component capability.
Critical electrical power assets have no access controls.	Access to buildings that house electrical power supplies to critical assets.	• Establish strict access control procedures for buildings and areas housing important system components. • Relocate important system components to secured areas. • Bury electric power lines or protect poles with anti-ram barriers.
Power lines share right-of-way with other key utilities.	Bridges, tunnels, and trenches often involve shared rights-of-way for electrical power that may contain other key utilities.	• Establish mitigation options, such as backup power or transferring mission to another location, based on loss of the right-of-way. • Establish agreements with local community to increase security or patrols for these locations during increased threat periods. • Be aware of maintenance or repair activities for other utilities in these locations.
Backup generation is insufficient.	Generators and uninterruptible power supplies are not large enough to support the critical asset in case of primary power loss or in case the location does not stockpile sufficient fuel to support the operational time frame during an electrical power loss.	• Determine critical asset needs and purchase backup generators accordingly. • Maintain at least minimum operational requirements for consumables (i.e., fuel). • Distribute critical asset operations to other backup power supplied locations.

Source: DOD, *Defense Critical Infrastructure Program: Infrastructure Resiliency Guide: Reduce Your Vulnerabilities and Make Your Infrastructure Stronger, Version 1.0* (May 2007).

Appendix III: Survey of DOD Critical Assets

United States Government Accountability Office

Survey of DOD Critical Assets

Introduction

The U.S. Government Accountability Office (GAO) is an independent, non-partisan legislative branch agency that assists Congress in evaluating how the federal government spends taxpayer dollars. GAO supports the Congress in meeting its constitutional responsibilities and to help improve the performance and ensure the accountability of the federal government for the benefit of the American people. GAO provides Congress with timely information that is objective, fact-based, nonpartisan, nonideological, fair, and balanced.

In response to a congressional mandate in the House Report on the *National Defense Authorization Act for Fiscal Year 2009*, Title XXVIII, Defense Critical Infrastructure Program, Report 110-652 (May 16, 2008), GAO is conducting a review of the Assurance of Electrical Power Supplies to DOD Critical Assets (GAO code 351266). The following critical asset was selected for this survey:

Please enter asset here:

Since you have been identified as a subject matter expert for this asset, we ask that you coordinate the completion of this survey with other officials as necessary and return one consolidated survey for this asset.

Follow-Up

After we receive your reply, we may call you to schedule a follow-up telephone interview if we need to clarify some answers in the survey.

Deadline

To assist us, we ask that you complete and return this survey **by June 5, 2009, via SIPRNet to ArtadiD@gao.sgov.gov.** Please return the completed survey by e-mail. Simply save this file to your classified computer desktop, hard drive, or disk and attach it to your e-mail.

Instructions for Completing This Survey

You can answer most of the questions easily by checking boxes or filling in blanks. A few questions request narrative answers. Please note that the space provided will expand to accommodate your answer. You may write additional comments at the end of the survey. We request that you provide the most recent information from no earlier than January 1, 2006.

- Please **use your mouse** to navigate throughout the survey by clicking on the field or check box you wish to fill in. **Do not** use the **"Tab" or "Enter"** keys as doing so may cause formatting problems.
- To select or deselect a check box, simply click or double click on the box.
- Please indicate the security classification of your narrative responses by writing (U) for "unclassified" or (S) for "SECRET" at the beginning of each entry or paragraph, as appropriate. Please limit your responses to Task Critical Asset information classified no higher than "SECRET" in accordance with the Defense Critical Infrastructure Program (DCIP) Security Classification Guide, May 2007.

Contact Information

Thanks in advance for taking the time to complete this survey. If you have any questions about the survey or security classification of your responses, please contact either:

David Artadi, *GAO Analyst-in-Charge*
Phone: (404) 679-1989
SIPRNet: ArtadiD@gao.sgov.gov

or

Lt Col Norman Worthen
Phone: (703) 693-7542
SIPRNet:: Norman.Worthen@js.pentagon.smil.mil

Thank you for your help.

Contact Information

1. Although several people may participate in the completion of this survey, we ask that you provide contact information below for the person coordinating the completion of the survey in case we need to follow-up with additional questions.

Name: _____
Rank: _____
Title: _____
Unit Name: _____
Base/Organization: _____
Commercial Phone #: (___) ___-____
E-mail: _____
SIPRNet: _____

Section A. Reliance on Electrical Power

Again, please enter the name of the asset **for which this survey is being completed.**

2. Does this asset require electrical power in order to function and support its military mission(s)? *(Mark ☒ only one response)*

☐ Yes
☐ No ➔ **SKIP TO QUESTION #62**

3. To what extent does this critical asset require electrical power to function? *(Mark ☒ only one response)*

☐ All of the time (continuous/constant)
☐ Most of the time
☐ About half of the time
☐ Less than half of the time
☐ None of the time No ➔ **SKIP TO QUESTION #62**

Please explain if necessary:

4. **Does this critical asset require supporting infrastructure, such as water; natural gas; heating, ventilating, and air conditioning (HVAC); or any other supporting utility to function?** *(Mark ☒ only one response)*

   ☐ Yes
   ☐ No ➔ **SKIP TO QUESTION #6**

5. **Does this critical asset's supporting infrastructure require electrical power to function?** *(Mark ☒ only one response)*

   ☐ Yes
   ☐ No

6. **From what source does this asset generally receive its *primary* electrical power supply?** *(Mark ☒ only one response)*

   ☐ Non-DOD electricity provider(s) or utility(ies) (e.g., the commercial power grid)
   Name of provider(s) or utility(ies):
   ☐ DOD-generated electricity supply based on fossil fuels (e.g., diesel-powered generators)
   ☐ DOD-generated electricity supply based on solar energy
   ☐ DOD-generated electricity supply based on geothermal energy
   ☐ DOD-generated electricity supply based on wind energy
   ☐ DOD-generated electricity supply based on biomass energy
   ☐ DOD-generated electricity supply based on nuclear energy

7. **Does this asset rely on an intermediate or transitional uninterruptible power supply (UPS) (i.e. a battery backup) to provide power in the event of an electrical power disruption?** *(Mark ☒ only one response)*

   ☐ Yes ➔ **How many minutes is the UPS expected to provide electrical power to the asset?** minutes
   ☐ No ➔ **Why not?**

8. Does this asset have a *back-up* power source, other than UPS, in the event of an electrical power disruption from any of the following sources? *(Mark ☒ one response for each row)*

Source	Yes	No
a. Batteries or fuel cells (other than UPS)	☐	☐
b. Non-DOD electricity provider(s)/utility(ies) (e.g., the commercial power grid) Name of provider(s) or utility(ies):	☐	☐
c. DOD-generated electricity supply based on fossil fuels (e.g., diesel-powered generators)	☐	☐
d. DOD-generated electricity supply based on solar energy	☐	☐
e. DOD-generated electricity supply based on geothermal energy	☐	☐
f. DOD-generated electricity supply based on wind energy	☐	☐
g. DOD-generated electricity supply based on biomass energy	☐	☐
h. DOD-generated electricity supply based on nuclear energy	☐	☐

9. How long, collectively, can back-up electrical power sources identified in question 8 provide electricity to the critical asset? *(Mark ☒ only one response)*

- ☐ Less than 24 hours
- ☐ Between 1 and 3 days (72 hours)
- ☐ More than 3 days up to 1 week
- ☐ Between 1 and 2 weeks
- ☐ Over 2 weeks
- ☐ Indefinitely (as long as fuel is available)

Section B. Back-Up Generators

10. Do the back-up electrical power sources identified in question 8 involve electrical power generators? *(Mark ☒ only one response)*

- ☐ Yes
- ☐ No ➔ **SKIP TO QUESTION #25**

11. Are back-up generators dedicated to the critical asset or shared with other critical assets or infrastructure? *(Mark ☒ only one response)*

- ☐ Dedicated to the critical asset
- ☐ Shared with other critical assets or infrastructure

12. Is the back-up generator(s) sufficient to maintain the critical asset and meet its mission(s) requirements?

☐ Yes
☐ No ➔ **SKIP TO QUESTION #25**

13. How many days can these generators function before requiring replenishing energy supplies (e.g., diesel fuel, natural gas, JP-8, etc.)?

_____ days

14. How many days would the energy supply that is currently stored at the installation or location of the critical asset be able to support these generators?

_____ days

15. How many days can these generators function before requiring *preventive* maintenance?

_____ days

16. How many days can these generators function before requiring *corrective* maintenance?

_____ days

17. Do you have another back-up generator that could be utilized while performing preventive or corrective maintenance on the primary generator?

☐ Yes
☐ No

18. How frequently are the generators identified in question 10 above subject to inspection and preventive maintenance to ensure that they function as intended?

_____

19. Do you conduct inspections and preventive maintenance to these generators as prescribed by schedule requirements?

☐ Yes
☐ No

20. How frequently are these generators subject to routine testing to ensure that they function as intended?

_____

21. What plans, if any, do you have to obtain additional energy supplies for these generators once currently stocked supplies run out?

22. What size (in terms of electricity production capacity, such as kilowatts) are these generators?

23. What are the electrical requirements (such as kilowatts) for the critical asset?

24. When was this electrical requirement last validated?

(date)

Section C. Unplanned Disruptions to Electrical Power

25. How many unplanned disruptions, if any, to this asset's primary electrical power sources have occurred between January 1, 2006, and December 31, 2008? *(Mark ☒ only one response)*

- ☐ Zero
- ☐ 1 to 5
- ☐ 6 to 10
- ☐ More than 10
- ☐ Unknown

26. When did the disruption(s) occur? *(List date(s) for each disruption)*

27. How long did each of these disruptions last?

28. Do you know the cause(s) for each disruption?

- ☐ Yes
- ☐ No ➔ **SKIP TO QUESTION #31**

29. What were the causes of each disruption?

30. What trends, if any, did you identify regarding causes of the disruptions?

31. How, if at all, did the disruption(s) affect the asset's mission(s)?

32. What actions, if any, did you take to mitigate the impact of the disruption(s) on the asset's mission(s)?

33. Is this asset incorporated into its electricity provider's/utility's reconstitution or restoration planning? *(Mark ☒ only one response)*

☐ Yes
☐ No
☐ Unknown

34. Have any cyber or computer-based attacks or probes occurred that have negatively affected the delivery of electrical power to the asset or its supporting infrastructure? *(Mark ☒ only one response)*

☐ Yes
☐ No ➔ **SKIP TO QUESTION #37**
☐ Unknown ➔ **SKIP TO QUESTION #37**

35. How did you determine that such cyber or computer-based attacks or probes occurred? *(Mark ☒ only one response)*

36. Who did you inform, if anyone, about the cyber or computer-based attacks or probes? *(Mark ☒ only one response)*

Section D. Assessments

37. Were any assessments conducted between January 1, 2006, and December 31, 2008, that specifically examined (1) the vulnerabilities of this asset to electrical power disruptions and/or (2) the risks of electrical power disruptions to this asset? *(Mark ☒ only one response)*

☐ Yes
☐ No ➔ **SKIP TO QUESTION #54**

38. What organization(s) conducted the assessment(s)?

39. What were the date(s) of the assessment(s)?

40. Did the assessment(s) consider vulnerabilities or risks up to one node (electrical power substation) nearest to the installation or location of the critical asset (i.e., "one node beyond the fence")? *(Mark ☒ only one response)*

☐ Yes
☐ No

41. Did the assessment(s) consider vulnerabilities or risks beyond one node (electrical power substation) nearest to the installation or location of the critical asset (i.e., more than "one node beyond the fence")? *(Mark ☒ only one response)*

☐ Yes
☐ No

42. Which of the following vulnerabilities or risks listed below were identified from the assessments? *(Mark ☒ one response for each row)*

Vulnerabilities or risks	Yes	No
a. The reliability and resiliency of a commercial or DOD installation's power grid.	☐	☐
b. The physical security of commercial and DOD electrical power infrastructures.	☐	☐
c. The cyber-security of commercial and DOD electrical power infrastructures.	☐	☐
d. The lack of back-up electrical generation capabilities (maintenance, testing, fuel supplies, etc.).	☐	☐
e. Single points of failure within commercial/DOD electrical power infrastructures.	☐	☐
f. The lack of contingency plans for addressing electrical power disruptions to critical assets.	☐	☐
g. Other vulnerability or risk ➔ **Please describe:**	☐	☐

43. What detail was provided about each vulnerability or risk identified in question #42 above?

Section E. Measures Taken

44. Were measures proposed or recommended to address or manage these vulnerabilities or risks? *(Mark ☒ only one response)*

☐ Yes
☐ No ➔ **SKIP TO QUESTION #54**

45. What measures were proposed or recommended to address or manage these vulnerabilities or risks?

46. At what level within DOD was the decision made to implement the recommended measure(s) or not implement the measure(s) and accept the risks?

47. What criteria, if any, were used in determining which measure(s) would be taken to address, manage, or accept vulnerabilities or risks (e.g., asset criticality, costs, staffing, technology, funding availability, time constraints, prior Base Realignment and Closure decisions, etc.)?

48. Was the decision made to implement the recommended measure(s) or not implement the measure(s) and accept the vulnerabilities or risks?

☐ Yes, implement recommended measure(s)
☐ No, decided not to implement the recommended measure(s) and accept the vulnerabilities or risks

49. Were measures selected for implementation?

☐ Yes
☐ No ➔ **SKIP TO QUESTION #54**

50. What were the estimated costs for implementing these measures?

51. Have these measures been implemented, scheduled for implementation, or not scheduled for implementation at this time? *(Mark ☒ for all that apply).*

☐ Been implemented ➔ **Please identify measure(s):**
☐ Been scheduled for implementation ➔ **Please identify measure(s):**
☐ Not scheduled for implementation at this time ➔ **Please identify measure(s):**

52. Which DOD major budget category was (or is being) used to implement these measures? *(Mark ☒ for all that apply).*

- ☐ Operations and Maintenance
- ☐ Military Personnel
- ☐ Procurement
- ☐ Research and Development
- ☐ Other (Please specify)
- ☐ Unknown

53. What DoD organizational level implemented (or is implementing) these measures? *(Mark ☒ for all that apply).*

- ☐ Host installation
- ☐ Higher headquarters
- ☐ Major command
- ☐ Combatant command
- ☐ Other (Please specify)
- ☐ Unknown

Section F. Coordination with Other Entities

54. Is this asset located within the United States?

- ☐ Yes
- ☐ No ➔ **SKIP TO QUESTION #57**

55. To what extent, if at all, did you or the host installation of this asset coordinate with U.S. electricity provider(s) to identify or address potential vulnerabilities or risks identified in question 42 above? *(Mark ☒ only one response)*

- ☐ Not at all ➔ **SKIP TO QUESTION #62**
- ☐ Some extent
- ☐ Moderate extent
- ☐ Great extent

56. What was the nature of the coordination with U.S. electricity providers?

57. Is this asset located outside the United States?

- ☐ Yes
- ☐ No ➔ **SKIP TO QUESTION #62**

58. Have there been any efforts to coordinate with host-nation governments and/or foreign-owned electricity providers to identify or address potential vulnerabilities or risks identified in question #40 above?

☐ Yes
☐ No ➔ **SKIP TO QUESTION #62**
☐ Unknown ➔ **SKIP TO QUESTION #62**

59. What was the nature of the coordination with the host-nation governments and/or foreign-owned electricity provider(s)?

60. Did you or the host installation of this asset coordinate with any other organizations or entities (other than U.S. electricity providers or host-nation governments and/or foreign-owned electricity provider(s)) to identify or address potential vulnerabilities or risks? *(Mark ☒ only one response)*

☐ Yes
☐ No-➔ **SKIP TO QUESTION #62**

61. With whom did you or the host installation of this asset coordinate?

Section G. Additional Information

62. Please provide any additional information about efforts to identify, assess, or address the vulnerabilities and risks associated with electrical power disruptions to this asset that may not have been addressed through the previous questions.

Appendix IV: Survey of DOD Critical Asset Missions

United States Government Accountability Office
Survey of DOD Critical Asset Missions

Introduction

The U.S. Government Accountability Office (GAO) is an independent, non-partisan legislative branch agency that assists Congress in evaluating how the federal government spends taxpayer dollars. GAO supports the Congress in meeting its constitutional responsibilities and to help improve the performance and ensure the accountability of the federal government for the benefit of the American people. GAO provides Congress with timely information that is objective, fact-based, nonpartisan, nonideological, fair, and balanced.

In response to a congressional mandate in the House Report on the *National Defense Authorization Act for Fiscal Year 2009*, Title XXVIII, Defense Critical Infrastructure Program, Report 110-652 (May 16, 2008), GAO is conducting a review of the Assurance of Electrical Power Supplies to DOD Critical Assets (GAO code 351266). The following critical asset was selected for this survey:

Please enter asset here:

Since the Joint Staff (J-34) has agreed to respond to the mission-related questions for this asset, we ask that the Joint Staff (J-34) coordinate the completion of this survey with other officials as necessary and return one consolidated survey for this asset.

Follow-Up

After we receive your reply, we may call you to schedule a follow-up telephone interview if we need to clarify some answers in the survey.

Deadline

To assist us, we ask that you complete and return this survey by **June 26, 2009**, to David Artadi via **SIPRNet** at **ArtadiD@gao.sgov.gov** or to Mark Pross via **JWICS** at **igproma@dodig.ic.gov**, as appropriate. Please return the completed survey by e-mail. Simply save this file to your classified computer desktop, hard drive, or disk and attach it to your e-mail.

Instructions for Completing This Survey

You can answer most of the questions easily by checking boxes or filling in blanks. A few questions request narrative answers. Please note that the space provided will expand to accommodate your answer. You may write additional comments at the end of the survey. We request that you provide the most recent information from no earlier than January 1, 2006.

- Please **use your mouse** to navigate throughout the survey by clicking on the field or check box you wish to fill in. **Do not** use the **"Tab" or "Enter"** keys as doing so may cause formatting problems.
- To select or deselect a check box, simply click or double click on the box.
- Please indicate the security classification of your narrative responses by writing (U) for "unclassified," (S) for "SECRET," or (TS) for TOP SECRET at the beginning of each entry or paragraph, as appropriate. However, please try to limit your responses to Task Critical Asset information classified no higher than "SECRET" in accordance with the Defense Critical Infrastructure Program (DCIP) Security Classification Guide, May 2007.

Contact Information

Thanks in advance for taking the time to complete this survey. If you have any questions about the survey, please contact:

David Artadi, GAO *Analyst-in-Charge*
Phone: (404) 679-1989
SIPRNet: ArtadiD@gao.sgov.gov.

Thank you for your help.

Section A. Background

Again, please enter the name of the asset **for which this survey is being completed.**

1. Within which DCIP defense sector(s), as identified in DOD Directive 3020.40, *Defense Critical Infrastructure Program (DCIP)*, is this asset? *(Mark ☒ all that apply.)*

- ☐ Defense Industrial Base (DIB)
- ☐ Financial Services
- ☐ Global Information Grid (GIG)
- ☐ Health Affairs
- ☐ Intelligence, Surveillance, and Reconnaissance (ISR)
- ☐ Logistics
- ☐ Personnel
- ☐ Public Works
- ☐ Space
- ☐ Transportation
- ☐ Unknown

2. Where is this asset physically located? *(Mark ☒ only one response)*

- ☐ At a military installation ➔ please specify name of installation:
- ☐ At a commercial facility ➔ please specify name of facility:
- ☐ At an industrial site ➔ please specify name of industrial site:
- ☐ At a stand-alone facility ➔ please specify name of facility:

3. What is the nearest city (and U.S. state or country) to this installation, facility, or site?

a. City:
b. State (only if in the U.S.):
c. Country (only if outside the U.S.):

4. Who owns the asset? *(Mark ☒ only one response)*

- ☐ DOD military service ➔ please specify:
- ☐ DOD combatant command ➔ please specify:
- ☐ Other DOD organization ➔ please specify:
- ☐ Other (non-DOD) U.S. government organization (federal, state, or local) ➔ please specify:
- ☐ U.S. private organization ➔ please specify:
- ☐ Foreign military organization ➔ please specify:
- ☐ Foreign government (nonmilitary) ➔ please specify:
- ☐ Foreign private company ➔ please specify:
- ☐ Other ➔ please specify:

5. Who primarily operates the asset during normal operational status? *(Mark ☒ all that apply.)*

- ☐ DOD military department ➔ please specify:
- ☐ DOD combatant command ➔ please specify:
- ☐ Other DOD organization ➔ please specify:
- ☐ Other (non-DOD) U.S. government organization (federal, state, or local) ➔ please specify:
- ☐ U.S. private organization ➔ please specify:
- ☐ Foreign military ➔ please specify:
- ☐ Foreign government (nonmilitary) ➔ please specify:
- ☐ Foreign private company ➔ please specify:
- ☐ Other ➔ please specify:

Section B. Mission(s), Combatant Command(s), and Military Service(s) Supported by Asset

6. Which military mission(s) does this asset support within DOD during normal operational status <u>other than those missions already described in the document that the Joint Staff (J-34) provided to GAO about the surveyed assets on November 19, 2008</u>? *(Please list and describe the mission(s) based on the "mission impact statements" and "mission essential tasks"—as defined in DOD Manual 3020.45, Vol. I, DOD Critical Asset Identification Process (Oct. 24, 2008)—that were used to designate this asset at its current DCIP critical asset classification.)*

7. **For the military missions identified in question #6, which DOD Unified Combatant Command(s) with regional responsibilities, if any, does this asset support?** *(Mark ☒ all that apply)*

   ☐ United States Africa Command (USAFRICOM)
   ☐ United States Central Command (USCENTCOM)
   ☐ United States European Command (USEUCOM)
   ☐ United States Northern Command (USNORTHCOM)
   ☐ United States Pacific Command (USPACOM)
   ☐ United States Southern Command (USSOUTHCOM)

8. **For the military missions identified in question #6, which DOD Unified Combatant Command(s) with functional responsibilities, if any, does this asset support?** *(Mark ☒ all that apply)*

   ☐ United States Joint Forces Command (USJFCOM)
   ☐ United States Special Operations Command (USSOCOM)
   ☐ United States Strategic Command (USSTRATCOM)
   ☐ United States Transportation Command (USTRANSCOM)

9. **For the military missions identified in question #6, which DOD military service(s), if any, does this asset support?** *(Mark ☒ all that apply)*

   ☐ United States Army
   ☐ United States Air Force
   ☐ United States Navy
   ☐ United States Marine Corps

10. **For the military missions identified in question #6, which other DOD agencies or organizations, if any, does this asset support?**

11. **Which non-DOD mission(s), if any, does this asset support during normal operational status?** *(Please include the names of the non-DOD organizations whose missions are supported by the asset.)*

12. **Please provide any additional information regarding the missions, combatant commands, and military services supported by the asset that may not have been addressed through the previous questions.**

Appendix V: Survey of Coordination Efforts for DOD Critical Assets

United States Government Accountability Office
Survey of Coordination Efforts for DOD Critical Assets

Introduction

The U.S. Government Accountability Office (GAO) is an independent, non-partisan legislative branch agency that assists Congress in evaluating how the federal government spends taxpayer dollars. GAO supports the Congress in meeting its constitutional responsibilities and to help improve the performance and ensure the accountability of the federal government for the benefit of the American people. GAO provides Congress with timely information that is objective, fact-based, nonpartisan, nonideological, fair, and balanced.

In response to a congressional mandate in the House Report on the *National Defense Authorization Act for Fiscal Year 2009*, Title XXVIII, Defense Critical Infrastructure Program, Report 110-652 (May 16, 2008), GAO is conducting a review of the Assurance of Electrical Power Supplies to DOD Critical Assets (GAO code 351266). The following critical asset was selected for this survey:

Please enter asset here:

Since ASD(HD&ASA)/DCIP Office has agreed to respond to the coordination-related questions for this asset, we ask that ASD(HD&ASA)/DCIP Office coordinate the completion of this survey with other officials as necessary and return one consolidated survey for this asset.

Follow-Up

After we receive your reply, we may call you to schedule a follow-up telephone interview if we need to clarify some answers in the survey.

Deadline

To assist us, we ask that you complete and return this survey by **June 26, 2009,** to David Artadi via **SIPRNet** at **ArtadiD@gao.sgov.gov** or to Mark Pross via **JWICS** at **igproma@dodig.ic.gov**, as appropriate. Please return the completed survey by e-mail. Simply save this file to your classified computer desktop, hard drive, or disk and attach it to your e-mail.

Instructions for Completing This Survey

You can answer most of the questions easily by checking boxes or filling in blanks. A few questions request narrative answers. Please note that the space provided will expand to accommodate your answer. You may write additional comments at the end of the survey. We request that you provide the most recent information from no earlier than January 1, 2006.

- Please **use your mouse** to navigate throughout the survey by clicking on the field or check box you wish to fill in. **Do not** use the **"Tab" or "Enter"** keys as doing so may cause formatting problems.
- To select or deselect a check box, simply click or double click on the box.
- Please indicate the security classification of your narrative responses by writing (U) for "unclassified," (S) for "SECRET," or (TS) for TOP SECRET at the beginning of each entry or paragraph, as appropriate. However, please try to limit your responses to Task Critical Asset information classified no higher than "SECRET" in accordance with the Defense Critical Infrastructure Program (DCIP) Security Classification Guide, May 2007.

Contact Information

Thanks in advance for taking the time to complete this survey. If you have any questions about the survey, please contact:

David Artadi, GAO *Analyst-in-Charge*
Phone: (404) 679-1989
SIPRNet: ArtadiD@gao.sgov.gov.

Thank you for your help.

Section A. Coordination with DOD DCIP Stakeholders

Again, please enter the name of the asset **for which this survey is being completed.**

1. To what extent has coordination taken place between the owner/custodian/operator of this asset with the following DOD DCIP stakeholders to identify and/or address potential vulnerabilities or risks involving electrical power disruptions? *(Mark ☒ one response for each row)*

DOD DCIP stakeholders	Not at all	Some extent	Moderate extent	Great extent
a. Military service(s) (*Specify service(s):* **)**	☐	☐	☐	☐
b. Combatant command(s) (*Specify command(s):* **)**	☐	☐	☐	☐
c. Defense Infrastructure Sector Lead Agent(s) (*Specify Agent(s):* **)**	☐	☐	☐	☐
d. ASD(HD&ASA)/DCIP Office	☐	☐	☐	☐
e. Joint Staff (J-34)	☐	☐	☐	☐
f. Mission Assurance Division/Dahlgren, VA	☐	☐	☐	☐
g. Defense Threat Reduction Agency (DTRA)	☐	☐	☐	☐
h. Other DOD DCIP stakeholder(s) (*Specify other stakeholder(s):* *)*	☐	☐	☐	☐

NOTE: If you answered "Not At All" to Question #1, skip to Question #4. Otherwise, continue to Question #2.

2. What was the nature of the coordination with these DOD DCIP stakeholders?

3. What impact, if any, did this coordination with these DOD DCIP stakeholders have on identifying and/or addressing potential vulnerabilities or risks to the asset?

Section B. Coordination with Non-DOD Entities

4. **To what extent has coordination taken place between DOD stakeholders and the U.S. Department of Homeland Security to identify and/or address potential vulnerabilities or risks involving electrical power disruptions to the asset?**

   ☐ Not at all ➔ **SKIP TO QUESTION #8**
   ☐ Some extent
   ☐ Moderate extent
   ☐ Great extent

5. **Which DOD stakeholder(s) were involved in these coordination efforts with the U.S. Department of Homeland Security?**

6. **What was the nature of the coordination with the U.S. Department of Homeland Security?**

7. **What impact, if any, did this coordination with the U.S. Department of Homeland Security have on identifying and/or addressing potential vulnerabilities or risks involving electrical power disruptions to the asset?**

8. **To what extent has coordination taken place between DOD stakeholders and the U.S. Department of Energy to identify and/or address potential vulnerabilities or risks involving electrical power disruptions to the asset?**

   ☐ Not at all *(Skip to question #12.)*
   ☐ Some extent
   ☐ Moderate extent
   ☐ Great extent

9. **Which DOD stakeholder(s) were involved in these coordination efforts with the U.S. Department of Energy?**

10. **What was the nature of the coordination with the U.S. Department of Energy?**

11. What impact, if any, did this coordination with the U.S. Department of Energy have on identifying and/or addressing potential vulnerabilities or risks to the asset?

12. To what extent has coordination taken place between DOD stakeholders and the U.S. Federal Energy Regulatory Commission (FERC) to identify and/or address potential vulnerabilities or risks involving electrical power disruptions to the asset?

- ☐ Not at all ➔ **SKIP TO QUESTION #16**
- ☐ Some extent
- ☐ Moderate extent
- ☐ Great extent

13. Which DOD stakeholder(s) were involved in these coordination efforts with the FERC?

14. What was the nature of the coordination with the FERC?

15. What impact, if any, did this coordination with the FERC have on identifying and/or addressing potential vulnerabilities or risks to the asset?

16. To what extent has coordination taken place between DOD stakeholders and the North American Electric Reliability Corporation (NERC) to identify and/or address potential vulnerabilities or risks involving electrical power disruptions to the asset?

- ☐ Not at all ➔ **SKIP TO QUESTION #20**
- ☐ Some extent
- ☐ Moderate extent
- ☐ Great extent

17. Which DOD stakeholder(s) were involved in these coordination efforts with the NERC?

18. What was the nature of the coordination with the NERC?

19. What impact, if any, did this coordination with the NERC have on identifying and/or addressing potential vulnerabilities or risks to the asset?

20. To what extent has coordination taken place between DOD stakeholders and DOE national laboratories to identify and/or address potential vulnerabilities or risks involving electrical power disruptions to the asset?

- ☐ Not at all ➔ **SKIP TO QUESTION #24**
- ☐ Some extent *(Specify laboratory(ies):)*
- ☐ Moderate extent *(Specify laboratory(ies):)*
- ☐ Great extent *(Specify laboratory(ies):)*

21. Which DOD stakeholder(s) were involved in these coordination efforts with DOE national laboratories?

22. What was the nature of the coordination with DOE national laboratories?

23. What impact, if any, did this coordination with DOE national laboratories have on identifying and/or addressing potential vulnerabilities or risks to the asset?

24. To what extent has coordination taken place between DOD stakeholders and the U.S. Department of State to identify and/or address potential vulnerabilities or risks involving electrical power disruptions to the asset?

- ☐ Not at all ➔ **SKIP TO QUESTION #28**
- ☐ Some extent
- ☐ Moderate extent
- ☐ Great extent

25. Which DOD stakeholder(s) were involved in these coordination efforts with the U.S. Department of State?

26. What was the nature of the coordination with the U.S. Department of State?

27. What impact, if any, did this coordination with the U.S. Department of State have on identifying and/or addressing potential vulnerabilities or risks to the asset?

28. To what extent has coordination taken place between DOD stakeholders and <u>electrical power industry associations</u> to identify and/or address potential vulnerabilities or risks involving electrical power disruptions to the asset?

☐ Not at all ➔ **SKIP TO QUESTION #32**
☐ Some extent *(Specify association(s):)*
☐ Moderate extent *(Specify association(s):)*
☐ Great extent *(Specify association(s):)*

29. Which DOD stakeholder(s) were involved in these coordination efforts with <u>electrical power industry associations</u>?

30. What was the nature of the coordination with <u>electrical power industry associations</u>?

31. What impact, if any, did this coordination have on identifying and/or addressing potential vulnerabilities or risks to the asset?

32. To what extent has coordination taken place between DOD stakeholders and <u>any other organizations not mentioned above</u> to identify and/or address potential vulnerabilities or risks involving electrical power disruptions to the asset?

☐ Not at all ➔ **SKIP TO QUESTION #26**
☐ Some extent *(Specify other organization(s):)*
☐ Moderate extent *(Specify other organization(s):)*
☐ Great extent *(Specify other organization(s):)*

33. Which DOD stakeholder(s) were involved in these coordination efforts <u>with these other organizations</u>?

34. What was the nature of the coordination with <u>these other organizations</u>?

35. What impact, if any, did this coordination with <u>these other organizations</u> have on identifying and/or addressing potential vulnerabilities or risks to the asset?

36. Please provide any additional information regarding coordination with DOD or non-DOD organizations to identify and/or address potential vulnerabilities or risks involving electrical power disruptions to the asset that may not have been addressed through the previous questions.

Appendix VI: Comments from the Department of Defense

Note: The cover letter for DOD's written comments indicates that the DOD Office of Security Review reviewed the draft report and recommended that the draft report be protected at the SECRET level. However, by deleting certain sections from the draft report, we were able to issue this unclassified report with the approval of the DOD Office of Security Review with a different report number.

HOMELAND DEFENSE
& AMERICAS' SECURITY AFFAIRS

ASSISTANT SECRETARY OF DEFENSE
2600 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-2600

OCT 6 2009

Ms. Davi M. D'Agostino
Director, Defense Capabilities and Management
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Ms. D'Agostino:

This is the Department of Defense (DoD) response to the GAO draft report, GAO-09-954C, "Defense Critical Infrastructure: Actions Needed to Improve the Identification and Management of Electrical Power Risks and Vulnerabilities to DoD Critical Assets," dated August 21, 2009 (GAO Code 351266). DoD concurs with the seven recommendations in the report. Our response to your recommendations is attached.

The DoD Office of Security Review has reviewed the report and recommends that the report be protected at the SECRET level.

Our point of contact for this action is Mr. Jamie Clark, Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (OASD (HD&ASA)), (703) 602-5730, Extension 142 or Jamie.Clark@osd.mil.

Sincerely,

Paul N. Stockton

Attachment:
As stated

GAO DRAFT REPORT – DATED AUGUST 24, 2009
GAO CODE 351266/GAO-09-954C

"DEFENSE CRITICAL INFRASTRUCTURE: Actions Needed to Improve the Identification and Management of Electrical Power Risks and Vulnerabilities to DoD Critical Assets"

DEPARTMENT OF DEFENSE COMMENTS TO THE RECOMMENDATIONS

RECOMMENDATION 1: The GAO recommends that the Secretary of Defense direct the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs, in collaboration with the Joint Staff's Directorate for Antiterrorism and Homeland Defense, combatant commands, military services, and other Defense Critical Infrastructure stakeholders, as appropriate, to complete Defense Critical Infrastructure Program vulnerability assessments, as required by DoD Instruction 3020.45, on all of DoD's most critical assets by October 2011.

DOD RESPONSE: Concur. The Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD (HD&ASA)) Defense Critical Infrastructure Program (DCIP) Office has been working closely with the Joint Staff, which is assigned responsibility for the implementation of vulnerability assessments in DoD Instruction 3020.45, to ensure that DCIP vulnerability assessments focus on DoD's most critical assets. The Joint Staff, in coordination with OASD (HD&ASA) has begun ensuring that these most critical assets are assessed utilizing an all-hazards and mission-assurance approach.

RECOMMENDATION 2: The GAO recommends that the Secretary of Defense direct the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs, in collaboration with the Joint Staff's Directorate for Antiterrorism and Homeland Defense, combatant commands, military services, and other Defense Critical Infrastructure stakeholders, as appropriate, to develop additional guidelines, an implementation plan, and a schedule for conducting vulnerability assessments on all non-DoD-owned most critical assets located in the United States and abroad in conjunction with other federal agencies, as appropriate, that have a capability to implement the plan.

DOD RESPONSE: Concur. The ASD (HD&ASA) DCIP Office has been working closely with the Joint Staff, which is assigned responsibility for the implementation of vulnerability assessments in DoD Instruction 3020.45, to ensure that DCIP vulnerability assessments focus on DoD's most critical assets. The Joint Staff, in coordination with OASD (HD&ASA) has begun ensuring that these most critical assets are assessed utilizing an all-hazards and mission-assurance approach, including the development of a self assessment capability. Non-DoD-

owned assets, especially those located abroad, require agreement of owners and present significant challenges. The ASD(HD&ASA) DCIP Office is coordinating with the appropriate offices to determine if remote assessments of these assets are possible.

RECOMMENDATION 3: The GAO recommends that the Secretary of Defense direct the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs, in collaboration with the Joint Staff's Directorate for Antiterrorism and Homeland Defense, combatant commands, military services, and other Defense Critical Infrastructure stakeholders, as appropriate, to establish a time frame for the military services to provide the infrastructure data required for the Public Works Infrastructure Sector Lead Agent-the U.S. Army Corps of Engineers-to conduct its preliminary technical analysis of public works (including electrical system) infrastructure at DoD installations that support DoD's most critical assets.

DOD RESPONSE: Concur. The ASD(HD&ASA) DCIP Office has been working closely with the U.S. Army Corps of Engineers (USACE), which is the lead agent for the Public Works Defense Sector, to ensure that proper characterization of critical assets is taking place from a public works perspective. The effort, while time intensive, has so far been successful and is on-going. The USACE has completed its characterization of public works infrastructure "outside the fence" for all of DoD's most critical assets, and is working with the Military Services to obtain information on the public works infrastructure "inside the fence."

RECOMMENDATION 4: The GAO recommends that the Secretary of Defense direct the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs, in collaboration with the Joint Staff's Directorate for Antiterrorism and Homeland Defense, combatant commands, military services, and other Defense Critical Infrastructure stakeholders, as appropriate, to finalize guidelines currently being developed to coordinate Defense Critical Infrastructure Program assessment criteria and processes more systematically with those of other DOD mission assurance programs.

DOD RESPONSE: Concur. DoD Directive 3020.40 acknowledges the existence of, and the synergistic effect of various complimentary risk management program activities and security related functions in its definition of Mission Assurance. The other activities respond to their own directives and appropriations, and several have their own assessment programs, but they have not yet been brought under a common mission assurance umbrella. Critical Infrastructure Protection (CIP) at the installation level is in its early stages and is not yet mature. For example, many of the positions dealing with CIP at the installation level are additional duties. The Joint Staff is overseeing a vulnerability assessment way ahead to better synchronize these efforts.

RECOMMENDATION 5: The GAO recommends that the Secretary of Defense direct the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs, in collaboration with the Joint Staff's Directorate for Antiterrorism and Homeland Defense, combatant commands, military services, and other Defense Critical Infrastructure stakeholders, as appropriate, to develop explicit Defense Critical Infrastructure Program guidelines for assessing the critical assets' vulnerabilities to long-term electrical power disruptions.

DOD RESPONSE: Concur. The ASD (HD&ASA) DCIP Office will review current vulnerability assessment criteria and standards and work with the Joint Staff to include considerations of long-term electrical power disruptions. Vulnerabilities are directly related to mission and its duration and the duration of the outage. A significant number of critical assets have back up power sources available in the event that commercial power is disrupted. As GAO noted in its report, 25 of the 34 assets surveyed reported that electrical power disruptions resulted in no or minimal impact to their missions. The Department is working on providing the same protection from commercial power disruption to the remaining assets.

RECOMMENDATION 6: The GAO recommends that the Secretary of Defense direct the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs, in collaboration with the Joint Staff's Directorate for Antiterrorism and Homeland Defense, combatant commands, military services, and other Defense Critical Infrastructure stakeholders, as appropriate, to develop a mechanism to systematically track the implementation of future Defense Critical Infrastructure Program risk management decisions and responses intended to address electrical power-related risks and vulnerabilities to DoD's most critical assets.

DOD RESPONSE: Concur. The ASD(HD&ASA) DCIP Office has developed a draft DoD Manual 3020.45 Volume 5, *Defense Critical Infrastructure Program (DCIP) Coordination Timeline,* currently in coordination within the Department. The purpose of the manual is to provide uniform procedures for the execution of DCIP activities and timelines that OASD (HD&ASA), the Joint Staff, Military Departments, Combatant Commands, Defense Agencies, and the Defense Infrastructure Sector Lead Agencies will use to coordinate the execution of activities and responsibilities assigned in DoD Directive 3020.40, DoD Instruction 3020.45, DoD Manual 3020.45 Volumes 1 and 2, and the resultant risk decision packages. The DCIP Office is also developing an automated CAIP Collaboration Tool that will document and track the status of each organization's progress as they work through the risk management process. The Collaboration Tool in conjunction with the Coordination Timeline will serve as a forcing function to ensure the accomplishment of tasks and to provide feedback to the components on status of actions, including electrical power-related risks and vulnerabilities.

RECOMMENDATION 7: The GAO recommends that the Secretary of Defense direct the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs, in collaboration with the Joint Staff's Directorate for Antiterrorism and Homeland Defense, combatant commands, military services, and other Defense Critical Infrastructure stakeholders, as appropriate, to ensure for DoD-owned most critical assets, and facilitate for non-DoD-owned most critical assets, that asset owners or host installations of the most critical assets, where appropriate, reach out to local electricity providers in an effort to coordinate and help remediate or mitigate risks and vulnerabilities to electrical power disruptions

DOD RESPONSE: Concur. In May 2007, the ASD(HD&ASA) DCIP Office promulgated the DCIP Infrastructure Resiliency Guide that provides information for improving the resiliency of infrastructure systems, networks, and solutions for reducing risks to infrastructure networks. The Department has identified the common vulnerabilities to infrastructure as a result of numerous infrastructure vulnerability assessments conducted by multiple agencies and organizations within the Department of Defense. The guide is a compilation of these findings and the resultant corrective actions. The guide contains a section devoted to electric power and provides guidelines to government and private-sector decision makers and those responsible for electric power supply, to ensure electric power disruptions do not adversely or unexpectedly affect mission accomplishment. The guide includes such actions as:

- Understand the requirements for electric power, how it is delivered, and the relative priority for restoring power;
- Ensure and maintain provider awareness of critical times when power is essential to mission execution;
- Work with the electric power providers to identify remedies to potential single points of failure.

On October 28, 2008, the ASD(HD&ASA) DCIP Office also promulgated DoD Manual 3020.45 Volume 2, *DCIP Remediation Planning* which describes a process for DoD leaders, once risk has been assessed, to determine, plan, justify, and implement remediation actions to reduce risk to defense critical infrastructure. The manual acknowledges that the DoD mission depends upon public infrastructure networks and services such as transportation, electric power, and communication networks. The manual advises the DoD facility managers to establish good communications with public service providers about service requirement, and to review service level agreements, acquisition programs, contracts, and operational processes for opportunities to address and include stronger resiliency language and requirements for future remediation efforts. This guidance will be reinforced at DCIP collaboration forums such as Defense Critical Infrastructure Integration Staff, Operational Advisory Board, and Defense Infrastructure Sector Council.

Appendix VII: GAO Contact and Staff Acknowledgments

GAO Contact

Davi M. D'Agostino, (202) 512-5431 or dagostinod@gao.gov

Acknowledgments

In addition to the contact named above, Mark A. Pross, Assistant Director; David G. Artadi; James D. Ashley; Yecenia C. Camarillo; Gina M. Flacco; Brian K. Howell; Katherine S. Lenane; Greg A. Marchand; Michael S. Pose; Terry L. Richardson; John W. Van Schaik; Marc J. Schwartz; and Cheryl A. Weissman made key contributions to this report.

Related GAO Products

Defense Critical Infrastructure Protection

Defense Critical Infrastructure: Actions Needed to Improve the Consistency, Reliability, and Usefulness of DOD's Tier 1 Task Critical Asset List. GAO-09-740R. Washington, D.C.: July 17, 2009.

Defense Critical Infrastructure: Developing Training Standards and an Awareness of Existing Expertise Would Help DOD Assure the Availability of Critical Infrastructure. GAO-09-42. Washington, D.C.: October 30, 2008.

Defense Critical Infrastructure: Adherence to Guidance Would Improve DOD's Approach to Identifying and Assuring the Availability of Critical Transportation Assets. GAO-08-851. Washington, D.C.: August 15, 2008.

Defense Critical Infrastructure: DOD's Risk Analysis of Its Critical Infrastructure Omits Highly Sensitive Assets. GAO-08-373R. Washington, D.C.: April 2, 2008.

Defense Infrastructure: Management Actions Needed to Ensure Effectiveness of DOD's Risk Management Approach for the Defense Industrial Base. GAO-07-1077. Washington, D.C.: August 31, 2007.

Defense Infrastructure: Actions Needed to Guide DOD's Efforts to Identify, Prioritize, and Assess Its Critical Infrastructure. GAO-07-461. Washington, D.C.: May 24, 2007.

Critical Infrastructure Protection

The Department of Homeland Security's (DHS) Critical Infrastructure Protection Cost-Benefit Report. GAO-09-654R. Washington, D.C.: June 26, 2009.

Influenza Pandemic: Opportunities Exist to Address Critical Infrastructure Protection Challenges That Require Federal and Private Sector Coordination. GAO-08-36. Washington, D.C.: October 31, 2007.

Critical Infrastructure: Sector Plans Complete and Sector Councils Evolving. GAO-07-1075T. Washington, D.C.: July 12, 2007.

Critical Infrastructure Protection: Sector Plans and Sector Councils Continue to Evolve. GAO-07-706R. Washington, D.C.: July 10, 2007.

Critical Infrastructure: Challenges Remain in Protecting Key Sectors. GAO-07-626T. Washington, D.C.: March 20, 2007.

Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics. GAO-07-39. Washington, D.C.: October 16, 2006.

Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors. GAO-03-233. Washington, D.C.: February 28, 2003.

Critical Infrastructure Protection: Commercial Satellite Security Should Be More Fully Addressed. GAO-02-781. Washington, D.C.: August 30, 2002.

Electrical Power

Electricity Restructuring: FERC Could Take Additional Steps to Analyze Regional Transmission Organizations' Benefits and Performance. GAO-08-987. Washington, D.C.: September 22, 2008.

Department of Energy, Federal Energy Regulatory Commission: Mandatory Reliability Standards for Critical Infrastructure Protection. GAO-08-493R. Washington, D.C.: February 21, 2008.

Electricity Restructuring: Key Challenges Remain. GAO-06-237. Washington, D.C.: November 15, 2005.

Meeting Energy Demand in the 21st Century: Many Challenges and Key Questions. GAO-05-414T. Washington, D.C.: March 16, 2005.

Electricity Restructuring: Action Needed to Address Emerging Gaps in Federal Information Collection. GAO-03-586. Washington, D.C.: June 30, 2003.

Restructured Electricity Markets: Three States' Experiences in Adding Generating Capacity. GAO-02-427. Washington, D.C.: May 24, 2002.

Energy Markets: Results of FERC Outage Study and Other Market Power Studies. GAO-01-1019T. Washington, D.C.: August 2, 2001.

Cybersecurity

Cybersecurity: Continued Federal Efforts Are Needed to Protect Critical Systems and Information. GAO-09-835T. Washington, D.C.: June 25, 2009.

Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk. GAO-09-661T. Washington, D.C.: May 5, 2009.

National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture. GAO-09-432T. Washington, D.C.: March 10, 2009.

Critical Infrastructure Protection: DHS Needs to Better Address Its Cybersecurity Responsibilities. GAO-08-1157T. Washington, D.C.: September 16, 2008.

Critical Infrastructure Protection: DHS Needs to Fully Address Lessons Learned from Its First Cyber Storm Exercise. GAO-08-825. Washington, D.C.: September 9, 2008.

Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability. GAO-08-588. Washington, D.C.: July 31, 2008.

Critical Infrastructure Protection: Further Efforts Needed to Integrate Planning for and Response to Disruptions on Converged Voice and Data Networks. GAO-08-607. Washington, D.C.: June 26, 2008.

Information Security: TVA Needs to Address Weaknesses in Control Systems and Networks. GAO-08-526. Washington, D.C.: May 21, 2008.

Critical Infrastructure Protection: Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies. GAO-08-64T. Washington, D.C.: October 31, 2007.

Critical Infrastructure Protection: Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies. GAO-08-113. Washington, D.C.: October 31, 2007.

Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain. GAO-07-1036. Washington, D.C.: September 10, 2007.

Critical Infrastructure Protection: DHS Leadership Needed to Enhance Cybersecurity. GAO-06-1087T. Washington, D.C.: September 13, 2006.

Critical Infrastructure Protection: Challenges in Addressing Cybersecurity. GAO-05-827T. Washington, D.C.: July 19, 2005.

Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities. GAO-05-434. Washington, D.C.: May 26, 2005.

Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors. GAO-04-780. Washington, D.C.: July 9, 2004.

Technology Assessment: Cybersecurity for Critical Infrastructure Protection. GAO-04-321. Washington, D.C.: May 28, 2004.

Critical Infrastructure Protection: Establishing Effective Information Sharing with Infrastructure Sectors. GAO-04-699T. Washington, D.C.: April 21, 2004.

Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems. GAO-04-628T. Washington, D.C.: March 30, 2004.

Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems. GAO-04-354. Washington, D.C.: March 15, 2004.

Posthearing Questions from the September 17, 2003, Hearing on "Implications of Power Blackouts for the Nation's Cybersecurity and Critical Infrastructure Protection: The Electric Grid, Critical Interdependencies, Vulnerabilities, and Readiness." GAO-04-300R. Washington, D.C.: December 8, 2003.

Critical Infrastructure Protection: Challenges in Securing Control Systems. GAO-04-140T. Washington, D.C.: October 1, 2003.

Combating Terrorism: Observations on National Strategies Related to Terrorism. GAO-03-519T. Washington, D.C.: March 3, 2003.

Critical Infrastructure Protection: Efforts of the Financial Services Sector to Address Cyber Threats. GAO-03-173. Washington, D.C.: January 30, 2003.

High-Risk Series: Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures. GAO-03-121. Washington, D.C.: January 2003.

Critical Infrastructure Protection: Significant Challenges Need to Be Addressed. GAO-02-961T. Washington, D.C.: July 24, 2002.

Critical Infrastructure Protection: Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information Systems. GAO-02-474. Washington, D.C.: July 15, 2002.

Critical Infrastructure Protection: Significant Homeland Security Challenges Need to Be Addressed. GAO-02-918T. Washington, D.C.: July 9, 2002.

Critical Infrastructure Protection: Significant Challenges in Safeguarding Government and Privately Controlled Systems from Computer-Based Attacks. GAO-01-1168T. Washington, D.C.: September 26, 2001.

Critical Infrastructure Protection: Significant Challenges in Protecting Federal Systems and Developing Analysis and Warning Capabilities. GAO-01-1132T. Washington, D.C.: September 12, 2001.

Critical Infrastructure Protection: Significant Challenges in Developing Analysis, Warning, and Response Capabilities. GAO-01-1005T. Washington, D.C.: July 25, 2001.

Critical Infrastructure Protection: Significant Challenges in Developing Analysis, Warning, and Response Capabilities. GAO-01-769T. Washington, D.C.: May 22, 2001.

Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities. GAO-01-323. Washington, D.C.: April 25, 2001.

Critical Infrastructure Protection: Challenges to Building a Comprehensive Strategy for Information Sharing and Coordination. GAO/T-AIMD-00-268. Washington, D.C.: July 26, 2000.

Critical Infrastructure Protection: Comments on the Proposed Cyber Security Information Act of 2000. GAO/T-AIMD-00-229. Washington, D.C.: June 22, 2000.

Critical Infrastructure Protection: "ILOVEYOU" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities. GAO/T-AIMD-00-181. Washington, D.C.: May 18, 2000.

Critical Infrastructure Protection: National Plan for Information Systems Protection. GAO/AIMD-00-90R. Washington, D.C.: February 11, 2000.

Critical Infrastructure Protection: Comments on the National Plan for Information Systems Protection. GAO/T-AIMD-00-72. Washington, D.C.: February 1, 2000.

Critical Infrastructure Protection: Fundamental Improvements Needed to Assure Security of Federal Operations. GAO/T-AIMD-00-7. Washington, D.C.: October 6, 1999.

Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences. GAO/AIMD-00-1. Washington, D.C.: October 1, 1999.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548